PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

"PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL ENTORNO EMPRESARIAL DE SOFT WAREHOUSE S.A."

AUTOR:

DAYANA LIZETH AMOGUIMBA SILVA

DIRECTOR: ING. FABIÁN DE LA CRUZ

QUITO, 2018

Índice de Contenido

Tabla de Figuras 4
1. Capítulo: Seguridad de la Información 5
1.1 Importancia de la Información 5
1.2 ¿Qué es la Seguridad de la Información? 6
1.3 Principios de la seguridad de la información 11
1.4 Importancia de la Seguridad de la información 12
1.5 Seguridad Informática VS Seguridad de la Información 13
1.6 Conceptos básicos en materia de seguridad 15
1.6.1 Vulnerabilidades 15
1.6.2 Amenazas 15
1.6.3 Ataques 16
1.7 Buenas prácticas, estándares y normas de la seguridad de la información 17
1.8 Estrategias de seguridad de la información 18
1.9 Plan de seguridad de la información 19
1.10 Requerimientos de seguridad de la información 20
1.11 Contraste entre COBIT 5 e ISO 27001 21
1.11.1 Pros y contras de COBIT 5 para la seguridad de la información 21
1.11.2 Pros y contras de la ISO 27001 para la seguridad de la información 21
1.11.3 Comparativa entre COBIT 5 e ISO 27001 22
2. Capítulo: Políticas de Seguridad de la Información 24
2.1 ¿Qué son los principios y políticas de seguridad de la información? 24
2.1.1 Características de las buenas políticas 24
2.1.2 Jerarquía de conceptos 25
2.1.3 Requisitos de las buenas políticas 26
2.1.4 ¿Qué es una política de seguridad de la información? 26
2.2 Importancia de las políticas en el programa de seguridad de la información. 27
2.2.1 Etapas de las políticas de seguridad 29
2.3 Políticas de seguridad de la información 31
2.3.1 Desafíos al momento de crear políticas de seguridad 31
2.3.2 Reglas de oro para crear políticas de seguridad efectivas 31
2.3.3 Causas de fallo de las políticas de seguridad 33
3. Capítulo: Entorno empresarial de Soft Warehouse S.A. 34
3.1 Identidad Corporativa 34
3.1.1 Misión 34

3.1.2 Visión 34
3.1.3 Características deseables de los profesionales de Soft Warehouse S.A. 34
3.1.4 Que es lo que no puede hacer un profesional de Soft Warehouse S.A. 34
3.1.3 Valores 35
3.1.4 Productos 35
3.2 Roles y responsabilidades del personal de seguridad de la información. 39
3.3 Situación actual de la organización 39
4. Capítulo: Desarrollo de la Propuesta de Políticas de Seguridad de la Información. .. 49
4.1 Justificación 49
4.2 Motivación 49
4.3 Indicaciones 50
4.3.1 Dominio 1: Políticas de seguridad de la información 50
4.3.2 Dominio 2: Organización de la seguridad de la información 50
4.3.3 Dominio 3: Seguridad de los recursos humanos 51
4.3.4 Dominio 4: Gestión de activos. 52
4.3.5 Dominio 5: Control de accesos 53
4.3.6 Dominio 6: Criptografía 54
4.3.7 Dominio 7: Seguridad física y ambiental 54
4.3.8 Dominio 8: Seguridad de operaciones 55
4.3.9 Dominio 9: Seguridad de las comunicaciones 56
4.3.10 Dominio 10: Adquisición, desarrollo y mantenimiento de los sistemas de información 56
4.3.11 Dominio 11: Relaciones con proveedores 57
4.3.12 Dominio 12: Gestión de incidentes en la seguridad de la información 58
4.3.13 Dominio 13: Aspectos de seguridad de la información en la gestión de la continuidad del negocio 58
4.3.14 Dominio 14: Continuidad 59
5. Capítulo: Conclusiones y Recomendaciones 60
Conclusiones 60
Recomendaciones 61
Bibliografía 63
Anexos 67
Introducción 67
PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - PSI 68
Glosario de Términos 106

Tabla de Figuras

Figura 1. Resumen de las Principales Tendencias Identificadas 9
Figura 2. Brecha de seguridad interna durante los últimos 24 meses..... 10
Figura 3. Brecha de seguridad externa durante los últimos 24 meses 10
Figura 4. Seguridad informática vs Seguridad de la información 14
Figura 5. Políticas, Planes y Procedimientos de Seguridad. 25
Figura 6. Identificación de la política de seguridad en el ciclo de vida del proceso de seguridad. 29
Figura 7. Módulos del producto FITBANK. 36
Figura 8.Módulos del producto FITCOOP. 37
Figura 9. Módulos del producto FITFENICIOS. 38
Figura 10. Estructura Comité Seguridad de la Información. 41

Tabla 1: Diferencias entre COBIT 5 y la ISO 27001, tomado de (Arora, 2017) 23

1. Capítulo: Seguridad de la Información

El presente capítulo aborda conceptos que son utilizados a lo largo del desarrollo de la disertación y brindan una idea que permite entender la seguridad de la información; también se dará a conocer la importancia de mantener segura la información dentro del sector empresarial para la prevención de amenazas.

1.1 Importancia de la Información

COBIT 5 define a la información como: "... Un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel muy importante." (ISACA, 2012)

Con esto se puede entender que la información es un activo importante para todo tipo de organización grande, mediana o pequeña, de tal manera que si este recurso está bien sustentado puede reducir los problemas de incertidumbre y puede determinar la calidad de las decisiones que se tomen.

Los directivos de las empresas constantemente toman decisiones importantes encaminadas a llevar al éxito a la empresa, tomando en cuenta que dicha información que usan debe ser útil como materia prima para el desempeño y organización de la misma.

Al ser la información un factor esencial que proporciona valor; las personas, organizaciones y estados han buscado formas de protegerlas, generando estándares, guías de buenas prácticas, procedimientos y sistemas de control; dando paso a la seguridad de la información que tiene como base el mantener tres principios (Confidencialidad, Disponibilidad e Integridad), durante todo el ciclo de vida de la información.

Según (Lapiedra Alcamí, 2011) , la buena información es la que proporciona valor y debe reunir las siguientes cualidades:

- Normalidad: La información relevante es aquella que tiene la capacidad de aumentar el conocimiento y reducir la incertidumbre con relación al problema que se va a tratar. Esta cualidad se considera decisiva.

- Exactitud: La información debe ser exacta para los directivos con relación al propósito buscado, cabe recalcar que la exactitud depende de la importancia de la decisión que se toma.
- Completa: La información completa abarca cada uno de los puntos clave del problema que se está tratando.
- Confianza en la fuente: La confianza en la fuente se incrementa cuando ésta ha sido digna de crédito en el pasado, se utilizan varias fuentes para incrementar la confianza.
- Puntualidad: La información debe ser trasmitida en el momento en que va a ser utilizada.
- Detalle: La información debe contener la mínima cantidad de detalle para una decisiva toma de decisiones.
- Comprensión: Si la información no es entendida no puede ser utilizada ni mucho menos puede añadir valor, la comprensión es aquella que transforma los datos en información.

1.2 ¿Qué es la Seguridad de la Información?

Para poder definir que es la seguridad de la información se tiene que tener claro el concepto de seguridad como: "… Una condición que resulta del establecimiento y mantenimiento de medidas de protección que permitan a una empresa cumplir su misión o funciones críticas a pesar de los riesgos que plantean las amenazas a su sistema de información. Las medidas de protección son una combinación de disuasión, prevención, detección, recuperación y corrección que deben formar parte del riesgo de la empresa en su enfoque de gestión como lo describe." (Glossary of Key Information Security Terms, 2013)

Se considera uno de los principios fundamentales de la privacidad, por lo cual si una empresa externaliza el manejo de la información o datos confidenciales debe tomar precauciones para evitar el uso inadecuado de la misma.

Según (Pearson, 2014), se deben tomar medidas para garantizar la seguridad, aplicando medidas técnicas y organizativas para la protección contra:

- Acceso o divulgación no autorizados: en particular cuando el tratamiento implica la transmisión de datos a través de una red.
- Destrucción: destrucción o pérdida accidental o ilegal.
- Modificación: alteración inapropiada.
- Uso no autorizado: todas las demás formas ilegales de procesamiento.

Mediante la corrección de cada uno de estos aspectos se puede cubrir aspectos físicos, administrativos y técnicos.

Por las consideraciones anteriores, "… La seguridad de la información, asegura la confidencialidad, disponibilidad e integridad de la información, así como los sistemas implicados en su tratamiento, dentro de una organización, como lo describe. " (ISO/ IEC 27000, 2016)

Según (ISO, 2013), la seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles deben ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que la se cumplen los objetivos específicos de seguridad y negocios de la organización

Una de las principales preocupaciones de las organizaciones con cultura de seguridad es proteger la información crítica y sensible por ese motivo la seguridad radica en la aplicación y gestión de controles adecuados que abarquen una amplia gama de amenazas con el fin de garantizar el éxito comercial del negocio, y minimizar el riesgo a consecuencia de los incidentes.

Según (Gómez Vieites, 2014), en un sistema informático se puede recurrir a la implantación de distintas técnicas y mecanismos de seguridad con el fin de prevenir cualquier daño o amenaza tales como:

- Identificación de usuarios y política de contraseñas.
- Control lógico de acceso a los recursos.
- Copias de seguridad. Centros de respaldo.
- Cifrado de las transmisiones.
- Huella digital de mensajes.

- Sellado temporal de mensajes.
- Utilización de la firma electrónica.
- Protocolos criptográficos.
- Análisis y filtrado del tráfico (cortafuegos).
- Servidores proxy.
- Sistema de Detección de Intrusiones (IDS).
- Antivirus, etcétera.

Se puede denotar que las amenazas que afectan a los principios de confidencialidad, integridad y disponibilidad, características fundaméntales para tener información segura, son tanto internas como externas. A pesar de los avances y aplicaciones enfocadas a este tema, muchas organizaciones alrededor del mundo siguen sufriendo de incidentes de seguridad que afectan su información y más sorprendente aún, es saber que alrededor del 50% de estos incidentes son ocasionados por empleados o exempleados de las mismas empresas como lo resalta (Heyman, 2015).

Nuevos incidentes relacionados con la seguridad surgen con frecuencia en la actualidad, y sobre todo dentro de las organizaciones donde no existen programas para el control de la seguridad de la información.

"…Las amenazas relacionadas con la seguridad se han convertido en no sólo más numerosas y diversas, sino también perjudiciales, como lo describe." (NIST, 2012).

Se puede resaltar algunos de los principales incidentes a lo largo de la historia:

- Según (FayerWayer, 2017) Heartland Payment Systems es un proveedor de procesamiento de pagos y tecnología que sufrió un ataque a la base de datos en marzo de 2008, provocando que se divulgaran 134 millones de tarjetas de crédito y débito.
- Según (FIS, 2017) Fidelity National Information Serviceses el proveedor global más grande del mundo dedicado a soluciones tecnológicas financieras que en el año 2007 sufrió el robo por parte del administrador de base de datos de 3,2 millones de registros de clientes incluyendo datos bancarios y tarjetas de crédito.

Debido al gran número de incidentes ocasionados por entes internos y externos el tema de seguridad de la información ha cobrado notoriedad en las diversas organizaciones, en el hogar y en el diario vivir.

Según (Deloitte, 2017), en su encuesta sobre tendencias de Cyber Riesgos y Seguridad de la Información en Latinoamérica que se llevó a cabo durante los meses de Enero y Mayo de 2016, las cuatro principales tendencias identificadas se presentan en la Figura 1.

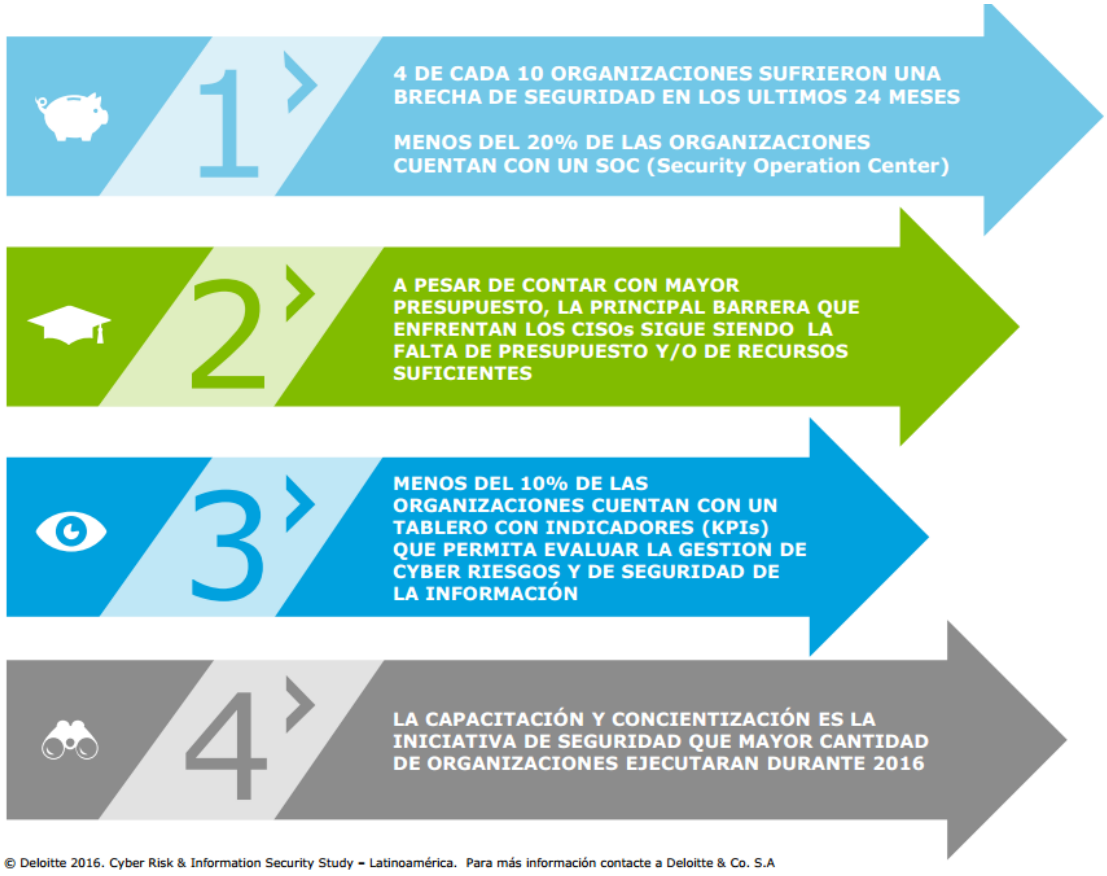

Figura 1. Resumen de las Principales Tendencias Identificadas
Fuente: La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información
Elaborado por: (Deloitte, 2017)

De acuerdo al estudio realizado, en la primera tendencia se puede denotar que las organizaciones siguen teniendo brechas de seguridad, lo cual nos da a entender que la inversión no solo debe estar destinada a implementar medidas de seguridad, sino también ocuparnos en el aspecto de las capacidades de monitoreo y la respuesta ante incidentes.

La segunda tendencia enfatiza la falta de recursos y presupuestos que se requieren para poder cubrir las necesidades y requerimientos de la organización.

En la tercera tendencia, menos del 10% no cuenta con indicadores[1] que permitan ver el riesgo al que está expuesta la organización, y sobre todo no hay conocimiento de los indicadores por parte de los empleados de la organización.

La cuarta tendencia es muy importante, puesto que si implementamos capacitación y concientización de los usuarios, adquiriremos conocimiento sobre los riesgos que podemos reducir.

En la Figura 2 se puede observar que la brecha de seguridad interna es del 70%, es un valor alarmante ya que se da a entender que no existe concientización por parte de los empleados y mucho menos controles de seguridad para aplacar los problemas.

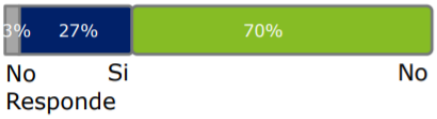

Figura 2. Brecha de seguridad interna durante los últimos 24 meses
Fuente: La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información
Elaborado por: (Deloitte, 2017)

El 62% presente en la Figura 3 corresponde a la brecha de seguridad dada por agentes externos a la organización.

Figura 3. Brecha de seguridad externa durante los últimos 24 meses
Fuente: La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información
Elaborado por: (Deloitte, 2017)

Es decir, que la solución de reducir problemas de seguridad de la información está en nuestras manos, generado una cultura de seguridad y creando un ambiente de seguridad dentro de la organización.

[1] Indicador: dato o información que sirve para conocer un hecho. Definición tomada de: The free Dictionary by Farlex

1.3 Principios de la seguridad de la información

Para que un sistema se pueda catalogar como seguro se debe garantizar que se cumplan los principios básicos de la seguridad de la información.

- Confidencialidad: la información exclusivamente debe ser accesible e interpretada por aquellos clientes y/o usuarios a los que está dirigida.

  Se debe tomar en cuenta que la vulneración de la confidencialidad afecta de diferente forma a equipos y redes de comunicación según (Seguridad informática, 2013):

  - Equipo de trabajo: Existe una violación de confidencialidad cuando un atacante tiene acceso a un equipo sin previa autorización, controlando todos sus recursos.
  - Red de comunicaciones: Existe una violación de confidencialidad cuando un atacante accede a los mensajes que circulan en la red sin tener previa autorización.

- Integridad: La información solo puede ser alterada por personal autorizado, independientemente de si esa modificación se produce de forma intencionada o no.

  Se debe tomar en cuenta que la vulneración de la integración afecta de diferente forma a equipos y redes de comunicación según (Seguridad informática, 2013):

  - Equipo de trabajo: Existe una violación de integridad cuando un usuario no legítimo realiza modificaciones de información del sistema sin tener previa autorización.
  - Red de comunicaciones: Existe una violación de integridad cuando un atacante actúa como intermediario en una comunicación que se esté realizando; recibe, modifica y envía al receptor.

- Disponibilidad: los usuarios y clientes deben tener acceso a la información en el momento que lo requieran.

  Se debe tomar en cuenta que la vulneración de la disponibilidad afecta de diferente forma a equipos y redes de comunicación según (Seguridad informática, 2013):

- Equipos informáticos: Existe una violación de disponibilidad cuando un usuario que posee accesos al sistema no puede utilizarlo.
- Red de comunicaciones: Existe una violación de disponibilidad cuando uno o varios recursos dejan de ser disponibles para otros usuarios que accedan al sistema.

Por lo tanto la seguridad de la información debe asegurar, promover y mantener cada uno de estos principios con el fin de salvaguardar la información.

1.4 Importancia de la Seguridad de la información

En la actualidad todas las personas, empresas u organizaciones a nivel mundial generan y captan una cantidad inmensa de datos y por ende información.

Según (Heyman, 2015), en la revista de "The New York Times" denota que alrededor de 1.7 trillones de fotos serán tomados en 2017, esto indica que la cantidad de información que se produce a nivel personal es mayor a la de cualquier momento en la historia porque vamos dejando un rastro digital de lo que hacemos, sin pensar que toda la información que producimos está corriendo riesgos de privacidad.

Tomando en cuenta el nivel empresarial, se tiene una relevancia de información con mayor magnitud, es por ello que estándares y guías de buenas prácticas han sido desarrollados en torno a la importancia de la información y el uso de tecnologías para aprovecharla y generar valor con su gestión.

Debemos tener en cuenta que a pesar de que nuestra empresa posea un amplio programa de seguridad, con el avance tecnológico que se ha ido dando en los últimos años, estamos abiertos a un número mayor de amenazas.

La importancia de la seguridad de la información no solo se aplica en ambientes relacionados con la tecnología sino en todo tipo de ambientes, es decir, si tomamos el ejemplo de un consultorio médico, el cual constantemente está albergando información de sus pacientes, el control de citas, medicamentos óptimos para los pacientes y una amenaza recae sobre esa información, el consultorio médico no podrá seguir funcionando, puesto que si la amenaza tergiversa la información, esto puede causar una mala administración de medicamentos, o un falso diagnóstico y el consultorio se vería afectado por la falta de confianza por parte de los pacientes.

Otro ejemplo se puede presentar en la manipulación de la información de un juzgado, si su información es vulnerable a ataques, los sentenciados tendrían otras condenas que no les pertenece por ende se estarían causando irregularidades penadas por la ley.

Estos y muchos casos son los que nos dan una idea de la responsabilidad que involucra tener segura nuestra información y sobretodo empezar a crear una cultura de seguridad dentro de la organización, de esa forma ir adoptando a la práctica diaria políticas de seguridad.

1.5 Seguridad Informática VS Seguridad de la Información

Es muy importante conocer cuál es la diferencia entre seguridad informática y seguridad de la información.

La seguridad de la información es todo aspecto relacionado con la protección de la información, pero entendiendo a la información o datos que están contenidos en algún medio sea o no digital, es decir como una lista de asistencia a una reunión en donde se colocan los nombres, cédula de identidad, dirección personal de correo electrónico, número de celular entre otros datos importantes, este es un activo físico de información.

Dentro de la compañía podemos realizar anotaciones de claves importantes y para no perderlas de vista las ponemos bajo el teclado o en nuestra libreta de notas, podemos realizar una firma de contratos y los dejamos sobre la mesa de escritorio, en cada uno de estas acciones tenemos como actor principal a la información la cual necesita ser resguardada. Es por eso que la seguridad de la información está relacionada en toda la organización, con todas las áreas que la conforman y cada uno de los empleados que la integran.

La seguridad informática es todo lo que abarca a la información que exclusivamente está comprendida en medios informáticos o digitales.

En la Figura 4, se denota que la seguridad informática está contenida dentro de la seguridad de la información.

Figura 4. Seguridad informática vs Seguridad de la información

La seguridad informática se encarga de proteger el sistema informático (SI) que comprende un conjunto de elementos físicos (hardware, dispositivos, periféricos, conexiones, etc.), lógicos (sistemas operativos, aplicaciones, etc.) y el elemento humano tratando de asegurar la integridad y privacidad de la información.

No obstante un sistema informático posee medidas de seguridad tales como:

- Cuáles son los elementos que componen el sistema mediante una retroalimentación a los responsables y directivos de la organización, de esta forma se obtendrá un estudio de los riesgos que se deben cubrir.
- Cuáles son los riesgos que afectan al sistema de maneras accidentales o provocadas.
- Cuáles son las medidas que se deben adoptar con el fin de reducir el riesgo al máximo.

Por lo tanto el objetivo fundamental de la seguridad informática es implantar medidas técnicas que preserven la infraestructura tecnológica y de comunicación dentro la organización.

Por otro lado en el campo de las organizaciones la seguridad de la información juega un papel fundamental en la implementación efectiva de la seguridad, ya que implica una gran interacción con otros departamentos.

La segregación de funciones es un concepto muy importante en la seguridad de la información. Si se separan las funciones, se reducen enormemente las posibilidades de que se utilicen indebidamente ciertos privilegios. Por ejemplo, si el rol de los administradores del sistema es crear cuentas de usuario y dar acceso a los usuarios del sistema y también garantizar un rendimiento óptimo de los sistemas. Toda esta actividad puede ser registrada y monitoreada por personal dedicado a hacer monitoreo del sistema.

Solo la colusión entre personas de los dos roles puede eludir la seguridad que brinda este enfoque.

Desde un punto de vista más amplio se define a la seguridad de la información como la preservación de la confidencialidad, integridad y su disponibilidad. Dependiendo del tipo de información que se maneje y de los procesos que se realicen en la organización, de tal manera que la seguridad de la información intenta proveer de medidas de seguridad sobre la información independientemente del medio en que esté, la seguridad informática únicamente se focaliza a la protección de las instalaciones informáticas y de la información en medios digitales.

1.6 Conceptos básicos en materia de seguridad

Dentro del mundo de la seguridad de la información es importante estudiar conceptos que se van a tratar en el transcurso de esta disertación.

1.6.1 Vulnerabilidades

"… Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados o provocado por una fuente de amenaza como lo describe." (NIST, 2013)

Este concepto resalta la importancia de corregir cualquier vulnerabilidad que sea detectada o descubierta, ya que afecta en la estabilidad y seguridad del sistema en general.

Las vulnerabilidades hacen que un atacante consiga privilegios, como por ejemplo los mismos que un administrador; logrando que acceda al sistema y pueda realizar acciones reservadas a estos.

1.6.2 Amenazas

"… Cualquier circunstancia o evento con el potencial de impactar adversamente operaciones organizacionales (incluyendo misión, funciones, imagen o activos organizativos, individuos, otras organizaciones o la nación) a través de un sistema de información vía acceso no autorizado, destrucción, revelación, modificación de información y / o denegación de servicio como lo describe." (NIST, 2013)

Se puede denotar que una amenaza también puede afectar al sistema de forma involuntaria, como, por ejemplo un desastre natural.

1.6.3 Ataques

"… Un intento de obtener acceso no autorizado a los servicios del sistema, recursos, o información, o un intento de comprometer la integridad del sistema como lo describe." (NIST, 2013)

Los ataques son por lo tanto acciones mal intencionadas que pueden llegar a poner en riesgo a un sistema.

Según (INCIBE, 2017) en el año 2016 se realizó una evaluación de los principales ataques de ciberseguridad producidos en 2016 en todo el mundo y recogidos a través de la Bitácora de Ciberseguridad de INCIBE[2] de los cuales citaré los tres más significativos:

- El robo de 81 millones de dólares al Banco Central de Bangladés perpetrado por piratas informáticos que lograron acceder a los sistemas informáticos del Banco y transferir esa cantidad de dinero a varios casinos de Filipinas. Un error ortográfico en el nombre de uno de los destinatarios levantó las alarmas evitando así el mayor robo de la historia, puesto que en realidad se habían realizado 35 peticiones para obtener casi 1.000 millones de dólares según (INCIBE, 2017).
- Robo de unos 64 millones de dólares en bitcoins[3] a la plataforma de intercambio Bitfinex de Hong Kong, el mayor operador mundial de intercambio de bitcoin basado en dólares, lo que provocó una caída de la cotización del bitcoin superior al 23 por ciento.
- Publicación de datos de 154 millones de votantes de Estados Unidos. Los datos incluían información personal como dirección, correo electrónico, número de teléfono o enlaces a redes sociales.

[2] INCIBE: Instituto Nacional de Ciberseguridad de España (INCIBE). Definición tomada de: https://www.incibe.es/

[3] Bitcoin: Es una moneda digital concebida en 2009. Definición tomada de: https://es.wikipedia.org/wiki/Bitcoin

1.7 Buenas prácticas, estándares y normas de la seguridad de la información

Es necesario buscar guías y documentos que nos sirvan de apoyo en la generación de políticas de seguridad, de esta forma podemos abordarla de forma responsable y procedimental con el objetivo de cumplir estándares mínimos requeridos. Es importante conocer el concepto de cada uno de los términos mencionados a continuación.

- Buena práctica: "…son una forma de homogeneizar la calidad con la que se trabaja a través de la estandarización." (Tus peores enemigos: las "best practices" y los estándares | Startups, Estrategia y Modelos de negocio, 2013)
- Estándar: "…Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido, y que ofrece reglas, guías o características para que se use repetidamente." (PMI, 2017)
- Norma: "…Una norma es un documento técnico contiene especificaciones técnicas de aplicación voluntaria, son elaborados por un consenso de las partes interesadas. Están basadas en los resultados de la experiencia y del desarrollo tecnológico." (Gestion Calidad, 2017)
- Marco de referencia: Según (Tcpsi, 2017)es un conjunto de métodos y prácticas que permiten establecer:
    - Criterios de información exigidos por los requisitos de negocio.
    - Procesos de negocio.
    - Recursos a utilizar.

A continuación se revisarán algunos estándares internacionales, guías y manuales de buenas prácticas que hoy en día están enfocados en seguridad de la información y en el aseguramiento de la misma.

ISO 27001:

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013 como lo describe (27001Academy, 2017).

Por medio de esta norma podemos determinar los requisitos óptimos para crear, implantar y realizar mejoras en un Sistema de Gestión de la Seguridad de la Información (SGSI) tomando como base el ciclo de Deming el cual posee los siguientes procesos: planificar, hacer, verificar y actuar.

ISO 27002:

Es una guía de buenas prácticas a partir de objetivos de control que sirve de base para que las organizaciones puedan implantar su Sistema de Gestión de la Seguridad de la Información (SGSI), para ello se definen políticas, procesos, procedimientos, estructuras organizativas y funciones tanto de software como de hardware. Una vez implantados, éstos deben ser revisados de forma constante con el fin de asegurar que son efectivos y ayudan a mitigar el riesgo.

ISO 27005:

Es una norma internacional que maneja la gestión de riesgos de la seguridad de la información, se puede implantar en todo tipo de organizaciones que tengan una visión de gestionar los riesgos que puedan afectar a la seguridad de la organización.

La norma provee directrices para la gestión de riesgos de seguridad de la información apoyado en los requisitos que están definidos en la ISO 27001.

COBIT 5:

Es un marco de referencia que aborda en uno de sus enfoques la seguridad de la información, generando un punto de partida para la creación de un sistema de Administración de Seguridad de la Información (ISMS) considerando algunos procesos que brindan una guía para operar y monitorear un sistema de seguridad; estos procesos son APO13: Gestionar la Seguridad, DSS04: Gestionar la continuidad y DSS05: Gestionar los servicios de seguridad.

COBIT 5 ayuda a las empresas a mitigar sus perfiles de riesgo por medio de una administración adecuada de la seguridad.

1.8 Estrategias de seguridad de la información

Según (Toolkit, 2017) propone las siguientes estrategias y alineamientos para la seguridad de la informacion.

- Concientizar a los/as usuarios/as sobre los aspectos de seguridad de la información

Es importante concientizar al personal acerca de temas relacionados con la seguridad de la información.

El personal debe asumir responsabilidades de acuerdo al trabajo que ejerce, es por eso que deben existir políticas claras y permanentes orientadas al personal.

- Definir los perfiles para los/as usuarios/as

Asignar permisos de acceso de acuerdo a las funciones y responsabilidades que realiza cada uno de los miembros del personal.

- Reforzar la seguridad de los sistemas

Es recomendable usar mecanismos de seguridad tales como: listas de accesos, firewall, traductor de direcciones de red (NAT)[4] entre otros con el fin de garantizar la seguridad.

- Efectuar copias de respaldos de la información

Es importante realizar copias de respaldo de la información y éstas deben guardarse en lugares seguros de preferencia en zonas externas a la organización, en el caso de que haya pérdida de datos o fallos en el sistema se puede recurrir a estas copias.

- Llevar a cabo un mantenimiento preventivo de los recursos tecnológicos

Se deben realizar el mantenimiento de los recursos tecnológicos permanente con el fin de analizar el estado de los equipos tanto de hardware como software.

Las estrategias que se citaron con anterioridad deben definir políticas, controles de seguridad que permitan contrarrestar amenazas que pongan en riesgo la integridad de las organizaciones.

1.9 Plan de seguridad de la información

Para realizar un plan de seguridad de la información se debe abordar un conjunto de dominios como sugerencias de la ISO 27002 y que debe estar contemplada por la administración general y deben ser comunicadas al personal activo de la empresa de una forma accesible y comprensible por el lector y a partes externas relevantes.

[4] NAT: permite el intercambio de paquetes de datos entre dos redes diferentes que se asignan mutuamente direcciones incompatibles. Definición tomada de: http://toolkit.cridlac.org/

La ISO 27002 recomienda utilizar un conjunto de mejores prácticas en la gestión de seguridad de la información y aborda ocho dominios importantes tales como:

- Políticas de seguridad: Revisión de las políticas para la seguridad de la información actuales.
- Organización de la seguridad de la información: Definir responsabilidades a los recursos inmersos en temas de seguridad de la información creando una estructura organizativa.
- Gestión de los activos: Trata de las responsabilidades que recaen sobre los activos (inventario, propiedad), la manipulación que se presta a la información y los manejos adecuados en el soporte de almacenamiento.
- Seguridad de los recursos humanos: Comprende el estudio de los antecedentes de los postulantes y la revisión de los términos que interfieren en el contrato, además de las medidas de seguridad que se toman en el caso de haber un despido o un cambio de puesto de trabajo.
- Seguridad física y del entorno: Trata sobre la seguridad de los equipos y protección, salida de activos fuera de las instalaciones, seguridad dentro de las oficinas, protección de amenazas externas y del medio ambiente.
- Gestión de comunicaciones: Comprende la seguridad de la red y la transferencia de información.
- Gestión de las operaciones: Trata sobre la monitorización y el control del software que se utiliza, coordinación de la auditoria de sistemas de información.
- Control de Acceso: Comprende la gestión de accesos que se brinda a los usuarios, control de accesos y responsabilidades de los usuarios.

1.10 Requerimientos de seguridad de la información

Según (ISO/IEC 27002, 2013), existen tres principales requerimientos de seguridad tales como:

- La evaluación de los riesgos de la organización; el conjunto de principios, objetivos y requisitos comerciales para el manejo, procesamiento, almacenamiento, comunicación y archivo que una organización ha desarrollado para respaldar sus operaciones

- Los requisitos legales, reglamentarios y contractuales; su negociación socios, contratistas y proveedores de servicios tienen que satisfacer y su entorno sociocultural
- El conjunto de principios, objetivos y requisitos comerciales para el manejo, procesamiento, almacenamiento, comunicación y archivo que una organización ha desarrollado para respaldar sus operaciones

1.11 Contraste entre COBIT 5 e ISO 27001

1.11.1 Pros y contras de COBIT 5 para la seguridad de la información

Como punto de partida hay que enfatizar que COBIT no solo abarca el tema de la seguridad de la información como tal, sino que es una guía y herramienta para la gestión y gobierno de las tecnologías de la información. COBIT 5 cuenta con 5 dominios y 37 procesos, de los cuales APO13: Gestionar la Seguridad, DSS04: Gestionar la continuidad y DSS05: Gestionar los servicios de seguridad están enfocados en la seguridad de la información.

La principal ventaja que presenta COBIT 5 para abordar la seguridad de la información es que posee un enfoque integral y holístico que comprende aspectos que las empresas suelen olvidar o no toman en cuenta, proporcionando habilitadores que ayudan a saber cuándo se requieren procesos, personal, recursos, entre otros. Además logra integrar la seguridad de la información dentro de la rama del marco de gestión de TI[5] ocasionando una mejor cobertura de la organización en este aspecto.

COBIT 5 está más orientado a los controles de TI que a la seguridad de la información en su totalidad, es por eso que la forma de implementar los aspectos de seguridad no son detallados con relación a qué medidas se deben tomar para mejorar la seguridad.

1.11.2 Pros y contras de la ISO 27001 para la seguridad de la información

La ISO 27001 es utilizada cuando se requieren estándares de administración de sistemas de seguridad de la información. Se basa en la mejora continua y requiere una revisión

[5] TI: conocida como tecnologías de la información, es la aplicación de ordenadores y equipos con el fin de almacenar, recuperar, trasmitir y manipulas dentro de negocios o empresas. Definición tomada de: https://es.wikipedia.org/wiki/Tecnolog%C3%ADa_de_la_informaci%C3%B3n

periódica para monitorear la seguridad sobre la información y poder tomar las medidas necesarias para abordar nuevos riesgos.

La principal ventaja de la ISO 27001 es que define prácticas y métodos para la implementación de la seguridad de la información detallando de forma clara cada uno de los controles mínimos requeridos. Proporciona una manera de asegurar la información por medio de un conjunto común de políticas, procedimientos y controles establecidos para administrar los riesgos a seguridad de información.

Al establecer la guía de buenas prácticas se requiere un esfuerzo continuo en el cual no hay retorno, es por eso que se debe mantener esta cultura de seguridad por parte de todos los integrantes de la organización, de lo contrario recaerá en los mismo errores que atentan con la integridad de la información.

1.11.3 Comparativa entre COBIT 5 e ISO 27001

La diferencia fundamental es que la ISO 27001 solo se enfoca en la seguridad de la información, mientras que COBIT se centra en controles de tecnología de información.

Para que una organización seleccione entre estos dos enfoques debe tener en mente la alineación de metas y objetivos que posea la misma, las relaciones con otras organizaciones, la capacidad para el logro de resultados, el presupuesto, la evolución y gestión de riesgos, el cuerpo de empleados entre otros.

La Tabla 1 hace una comparación y contraste entre COBIT 5 e ISO 27001 estipulado en el informe de “Comparing Different Information Security Standards” por (Comparing different information security standards: COBIT vs ISO 27001, 2017), donde se analizan los diferentes paradigmas, alcance y enfoque.

	COBIT 5	ISO 27001
Paradigma	Planificar los procesos de TI.	Sistema de Administración de seguridad de la información.
Alcance	Gobierno de TI de la organización incluyendo la planificación de seguridad. Es una solución íntegra.	Orientación independiente para la seguridad.
Enfoque	Orientación empresarial y gobierno de TI en su totalidad.	Implementación de controles de seguridad, énfasis en el enfoque de gestión de riesgos.
Modelo organizacional	Todos los interesados.	Gerencia, departamentos de sistemas de la información.

Tabla 1: Diferencias entre COBIT 5 y la ISO 27001.
Elaborado por: (Arora, 2017)

En la Tabla 1 se hace notar que son enfoques distintos, sin embargo los dos tienen como objetivo fundamental solventar los mismo problemas se seguridad de la información. COBIT 5 está más centrado en el gobierno de TI mientras que la ISO se enfoca esencialmente en la seguridad. De acuerdo al modelo organizacional de cada uno de los enfoques, se enfatiza que la ISO 27001 recae desde la gerencia y departamentos de sistemas de la información.

2. Capítulo: Políticas de Seguridad de la Información

El presente capítulo aborda el concepto básico de política, su importancia y las características que debe tener, además da una apertura al campo de las políticas de seguridad, brindando una serie de reglas para la construcción de las políticas.

2.1 ¿Qué son los principios y políticas de seguridad de la información?

Las políticas son instrumentos que nos permiten comunicar las reglas de la empresa.

Según (ISACA, 2012), las políticas deben tener un mecanismo (marco de referencia) establecido lo que permite que puedan ser administradas de forma eficaz y donde los usuarios puedan saber a dónde ir, por lo cual éstas deben ser:

- Integrales, que abarquen todas las áreas necesarias.
- Abiertas y flexibles, permitiendo su adaptación a la situación específica de la empresa.
- Actualizadas, que reflejan la dirección y objetivos de gobierno actuales de la empresa.
- Disponibles y accesibles a todas la partes interesadas.

Para COBIT 5 se debe realizar un manejo correcto, para ello resulta necesario hacer uso de un Framework (marco) de políticas, el cual debe cubrir los siguientes puntos:

- Personal que aprueba las políticas de la organización.
- Las consecuencias por fallar el cumplimiento de una política.
- Formas de manejar excepciones a las políticas.
- Medios por los que se revisará y medirá el cumplimiento de las políticas.

De acuerdo a lo anterior se pude definir que el propósito de un ciclo de vida de políticas es que debe respaldar un marco de referencia, con el objetivo de poder alcanzar los objetivos deseados.

2.1.1 Características de las buenas políticas

Estas deben ser:

- Eficaces: Lograr su propósito.

- Eficientes: Implementadas de forma eficiente.
- No intrusivas: Deben poseer sentido y lógica para las personas que tienen que cumplir con ellas.

2.1.2 Jerarquía de conceptos

Dentro del campo de seguridad se debe resaltar una jerarquía de conceptos al hablar de políticas, principios, y procedimientos de seguridad.

Figura 5. Políticas, Planes y Procedimientos de Seguridad.

Elaborado por: (Vieites, 2014)

De acuerdo a la Figura 5, en la cúspide de la pirámide se posicionan los objetivos fundamentales de la Gestión de la Seguridad de la Información y su equivalente a la confidencialidad, integridad y disponibilidad de la información.

Cuando se fijan los objetivos fundamentales de acuerdo a la organización se procede a definir las políticas de seguridad, así como planes de seguridad que abarca un conjunto de decisiones que definen acciones futuras y medios que se van a emplear y los procedimientos de actuación para la implantación en la organización.

Los procedimientos de seguridad es la base para implementar las políticas de seguridad, puesto que estas describen cuales son las actividades que se tienen que realizar en el sistema de acuerdo a las tareas y operaciones, en que momento o lugar, cuales son los responsables, cuales son los controles que se aplican para una correcta ejecución. Para poder crear políticas de seguridad efectivas se debe tener en cuenta las evidencias y

registros que posee la organización de esta forma se puede abordar el riesgo de mejor manera.

2.1.3 Requisitos de las buenas políticas

- Definir su alcance, es decir limitar de donde a donde va.
- Establecer las consecuencias de no cumplir con la política.
- Manejar medios de control de excepciones, es decir que todo cambio que se realice debe ser registrado y aprobado.
- Analizar cómo se realizará la monitorización de cada política.

2.1.4 ¿Qué es una política de seguridad de la información?

Una política de seguridad define y documenta la posición establecida de la organización frente a los riesgos de seguridad que se deben controlar. A menudo se considera que una política de seguridad es un "documento vivo", lo que significa que el documento nunca se termina, sino que se actualiza continuamente a medida que cambian los requisitos de la tecnología y los empleados.

La política de seguridad de una compañía puede incluir una política de uso aceptable, una descripción de cómo la compañía planea educar a sus empleados sobre la protección de los activos de la compañía, una explicación de cómo se llevarán a cabo y se aplicarán las medidas de seguridad y un procedimiento para evaluar la efectividad de la política de seguridad para asegurar que se harán las correcciones necesarias como lo resalta (Moore, 2015). De acuerdo a ello, se puede decir que cuando una política de seguridad mantiene un perfil demasiado restrictivo, o el detalle es escrito de forma inadecuada, es probable que sea violada.

Es un error encargar a una sola persona la creación del documento de políticas y sobre todo mantenerlo aislado del resto de la organización, de esta manera es imposible tener políticas exitosas y eficaces, la clave según Rob McMillan director de investigación de Gartner está en que “Los resultados exitosos de las políticas casi siempre requieren un proceso de consulta e iteración antes de que se elabore una posición final de política sostenible”

2.2 Importancia de las políticas en el programa de seguridad de la información.

Cuando se realicen las políticas de seguridad es sustancial que se comprenda la razón del por qué se están creando las políticas, ya que se requiere un apoyo universal, en primer lugar debe existir la disposición de los empleados para colaborar con la creación de las mismas otorgándoles derechos y responsabilidades. Una crítica común que suele suscitarse es que a menudo a las personas que trabajan en la organización se les comunica lo que no pueden hacer pero rara vez se les comunica lo que pueden hacer, es por eso que una alternativa eficaz es establecer una serie de escenarios reales a los que cada miembro del personal se enfrente y determinar como la política lo puede respaldar o impedir.

Como un segundo aspecto, es importante asegurar que todos los empleados conozcan sus propias responsabilidades para poder mantener la seguridad en la organización. Es difícil que una política de seguridad se pronostique a todas las amenazas del entorno, sin embargo, las políticas aseguran que para cada problema que se suscite dentro de la organización exista un responsable que pueda manejar el percance.

Las políticas de seguridad a menudo son escritas por personas que poseen conocimiento, sobre todo experiencia en seguridad pero no experiencia en políticas, a pesar de la gran cantidad de recursos que existen para redactar políticas, actualmente las empresas todavía tiene dificultades para mantener un enfoque de protección ante los riesgos.

Uno de los mayores riesgos que se puede resaltar es la toma de datos confidenciales por parte de los empleados cuando se van de la organización, según John Lane, CISO[6] de Biscom[7] destaca que los empleados son un gran agujero de seguridad, en la encuesta realizada a fines del 2015 por dicha empresa se encontró que el 87% de los empleados quienes trabajaban en la empresa tomaron datos de la empresa que crearon durante el trabajo, alrededor del 95% de los encuestados dijeron que tomar datos que no crearon fue posible porque su empresa no tenía políticas o tecnología para evitar el robo de datos o ignoraba sus políticas, y el 25% tomó propiedad intelectual.

[6] CISO: persona encargada de alinear las iniciativas de seguridad de la información y los objetivos del negocio.
Definición tomada de: http://searchdatacenter.techtarget.com/es/definicion/CISO-director-de-seguridad-de-la-informacion

[7] Biscom: es una empresa privada de software empresarial, líder mundial en el intercambio seguro de archivos. Definición tomada de: https://www.biscom.com/

Se puede decir que el robo de información daña a la organización en un sinnúmero de formas, obligando a la misma a tomar medidas de acción contra los ex empleados impactando negativamente a sus ingresos. Para poder reducir el riesgo se deben establecer políticas detalladas, garantizar la visibilidad de las prácticas de los empleados, limitar el acceso a los datos, cifrado de datos confidenciales, asegurar que haya un buen respaldo de datos para evitar pérdidas de información como lo sugiere (Osterman Research, Inc, 2016).

Según Rob McMillan, director de investigación de Gartner resalta que si no puede traducir sus requisitos en una política eficaz, entonces tiene pocas esperanzas de que sus requisitos se cumplan de manera exigible. Pero si lo haces bien, marcará una gran diferencia en la capacidad de tu organización para reducir el riesgo.

Las políticas de seguridad de la información varían de organización en organización, teniendo en cuenta que las políticas internas son útiles tanto para organizaciones pequeñas como grandes.

La siguiente lista de políticas sirve de soporte dentro de un programa de seguridad de la información, para lograr un control de seguridad de la información denotando las cuatro primeras políticas y el resto constituyen a otras áreas de la organización según lo resalta COBIT 5.

- Política de Control de Acceso
- Política de Seguridad de Información del Personal
- Política Física y ambiental de Seguridad de Información
- Política de respuesta a Incidentes de Seguridad
- Política de Continuidad del Negocio y Recuperación de Desastres
- Política de Administración de Activos
- Política de Comportamiento
- Políticas de Mantenimiento, Desarrollo y Adquisición de sistemas de Información
- Política de Administración de Proveedores
- Política de Administración de Operaciones y Comunicación
- Política de Cumplimiento de Normas
- Política de Administración de Riesgos

2.2.1 Etapas de las políticas de seguridad

Según (Areitio, 2008), existen cinco etapas que permiten la construcción de sus elementos generales:

- Objetivos de la política:
  En este elemento se deben brindar los detalles de a quién, cuándo y dónde se aplica la política de seguridad, con el fin de explicar de manera detallada los resultados esperados por el documento de políticas de seguridad.

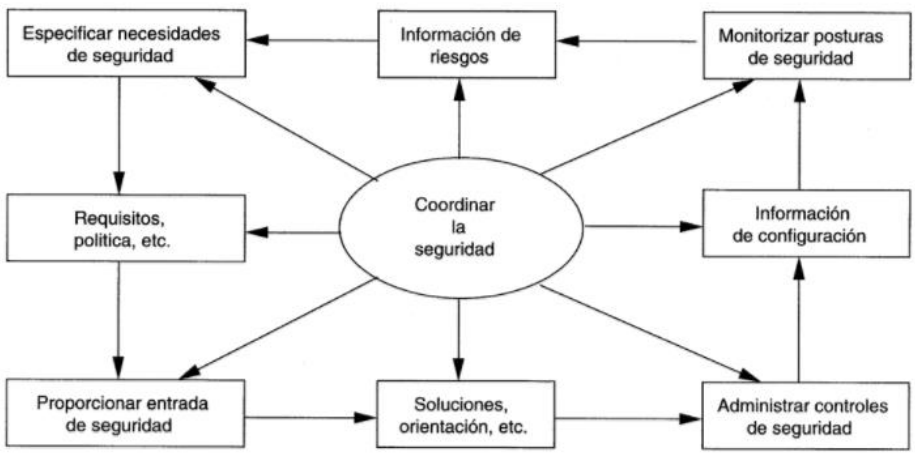

Figura 6. Identificación de la política de seguridad en el ciclo de vida del proceso de seguridad. Elaborado por: (Areitio, 2008)

De acuerdo a las Figura 6, la identificación de la política de seguridad puede empezar arbitrariamente en cualquiera de las fases puesto que es un proceso iterativo.

Para coordinar la seguridad es necesario especificar las necesidades de la misma; realizando una especificación de las necesidades de seguridad donde se incluyen los problemas actuales de seguridad que se deben cubrir, las necesidades de cada uno de los empleados frente a la falta de seguridad, entre otras.

Es necesario abordar cada uno de los factores que en base a los requisitos que se obtienen, formular políticas que ayuden a optimizar el riesgo, teniendo en cuenta las entradas de seguridad que actualmente posee la empresa para direccionarla a un nivel de mejora en base a soluciones.

Además se considera mantener una correcta administración de los controles de seguridad para poder analizar en base a un monitorio y seguimiento el progreso de cada una de las

políticas para una respectiva retroalimentación conjunta, los controles aislados y separados no son eficientes puesto que estos deben ser verificados para constatar que están funcionando y que está brindando la protección que se requiere a la empresa, finalmente se mejoran.

Al coordinar la seguridad debemos conocer la información de configuración de esta forma el personal seleccionado para distintas áreas sabrá los modos de accesos que se aplican sin provocar un mal uso de esta medida con el fin de asegurar la integridad de la información.

Cuando monitorizamos la seguridad nos permite visualizar el estado actual de la organización y encontrar incidentes o riesgos de forma preliminar, facilitando su atención en un tiempo adecuado.

La información de riesgos es muy importante porque en base a esto podemos conocer donde hay mayor impacto de pérdida de información, donde hay mayor probabilidad de que se pierda confidencialidad, integridad y disponibilidad. Conociendo cada uno de los posibles riesgos podemos tener un plan de contingencia para prevenirlos.

- Ámbito de la política

Este elemento nos brinda una descripción detallada del ambiente donde trabajará la política, es decir que se deben definir los aspectos que cubre, los sistemas que serán utilizados, la arquitectura del sistema o el hardware o software.

- Procedimientos de seguridad a adoptar

Este elemento trata las vulnerabilidades del negocio y las amenazas que se hayan identificado, así como las medidas que se han adoptado para manejar los riesgos. El objetivo de tratar las cuestiones de políticas de seguridad es para crear conciencia en los empleados.

- Reglas, regulaciones y normas para los empleados

En este elemento se debe manejar claramente los accesos al sistema y se establecerán los derechos de autorización para cada uno de los empleados.

Se aplicarán reglas para el uso adecuado de los medios electrónicos, en el caso en el que se esté dando un mal uso del mismo se deben tomar acciones disciplinarias correspondientes. Las reglas y regulaciones se deben hacer de manera cuidadosa con el

fin de que los empleados se sientan cómodos con la sanción, ya que si no optarán por hacer caso omiso a la misma.

- Gestión de la seguridad

En este elemento se debe explicar la forma en la que todos los empleados de la organización desde los directivos hasta los administrativos puedan contribuir con el mantenimiento de la seguridad de la información y se puedan definir los responsables de la administración de la seguridad.

2.3 Políticas de seguridad de la información

2.3.1 Desafíos al momento de crear políticas de seguridad

El uso de buenas prácticas brindan soporte para la planificación y redacción de políticas con el fin de hacer la diferencia en su efectividad y reducción de riesgos, es por ellos que al momento de crear políticas se seguridad se presentan algunos de los siguientes desafíos.

Según (Gartner, 2017):

- Una política rígida elimina innecesariamente su capacidad de considerar múltiples opciones para problemas complejos o difíciles.
- Las políticas mal redactadas pueden presentar problemas tales como posiciones de política inconsistentes, la incapacidad para garantizar el cumplimiento, perfiles de alto riesgo inaceptables o costos innecesariamente altos.
- Las políticas de seguridad que no se adaptan a los cambios en el entorno empresarial o en el entorno externo se volverán obsoletas y restringirán el desarrollo del negocio.

2.3.2 Reglas de oro para crear políticas de seguridad efectivas

- Crear un proceso para desarrollar y mantener su política.
  El desarrollo de políticas de seguridad se debe tomar como un proceso.
  El proceso debe abordar un pequeño cuerpo de políticas necesarias para la organización y construir sobre esa base las demás durante un período de años, lo cual resultará de eso un cuerpo de prácticas efectivas.

Según (Gartner, 2017), enfatiza que si no puedes defender tu proceso, entonces no podrás defender tu política puesto que las políticas se ejecutan a través de los procesos.

Se considera un error hacer que una persona con pleno conocimiento redacte un documento de políticas de seguridad de manera aislada. Los resultados exitosos de crear políticas de seguridad requieren un proceso de consulta e iteración continua antes de que se elabore una política definitiva.

Una vez que las políticas se publiquen en el entorno empresarial se deberá realizar una evaluación al menos anual. Esta revisión debe incluir una consulta tanto para las partes internas como externas de la organización, con el objetivo de revisar los problemas que surgieron.

- Utilizar un enfoque estructurado para respaldar la flexibilidad

  Se considera que las políticas deben ser sumamente flexibles para poder abordar el riesgo sin comprometer a toda la organización. Si se establecen políticas rígidas, poco flexibles en su enfoque o una política que no implica controles de seguridad fuertes no se llevará a cabo una gestión del riesgo adecuada.
- No desarrolle su política en aislamiento; desarrollar soporte mediante un proceso de compromiso

  Las políticas requieren un apoyo universal, es importante acudir a cada uno de los empleados de la organización para presenciar en tiempo real sus actividades de trabajo y analizar de forma objetiva como el desempeño de su trabajo se ve afectado por la política, de esta manera tanto el empleado como el encargado del seguimiento aportaran ideas de mejora. Una vez aprobada la política no pueden existir quejas o desacuerdos, esta es una parte del proceso de conciencia y educación para crear un ambiente de seguridad y conocimiento.
- Mantener una buena redacción de políticas

  Es inútil redactar un documento extenso que nadie leerá, hay que reconocer que la lectura del mismo demanda tiempo y nivel de atención alta, es por eso que una buena técnica involucrarnos en la redacción haciendo aportes al mismo, de esta forma no existirá resistencia por parte de los empleados y comprenderán porque es necesario aplicar políticas dentro de la organización.

2.3.3 Causas de fallo de las políticas de seguridad

Entre las causas más habituales de fallo de las políticas de seguridad se pueden denotar las siguientes:

- Falta de apoyo por parte de los empleados.
- Las políticas de seguridad no reflejan los objetivos de negocio de la organización.
- Inadecuada aplicación y control de las políticas de seguridad.
- Implicaciones legales y económicas.
- Falta de mantenimiento a las políticas de seguridad.

Hay que denotar que las políticas de seguridad deben establecer que información debe protegerse, quien tendrá acceso a la misma y el grado de seguridad que se requiere para cumplir los objetivos de negocio.

3. Capítulo: Entorno empresarial de Soft Warehouse S.A.

El presente capítulo aborda la identidad corporativa de Soft Warehouse S.A., además de los productos que ofrece a sus clientes. Se aborda la situación actual en base a los controles seguridad de la información que emplea la ISO 27001.

3.1 Identidad Corporativa

3.1.1 Misión

Comercializar, Vender, Implantar y Soportar Soluciones Informáticas creadas por la compañía utilizando siempre la mejor y más moderna tecnología disponible. Manteniéndolas permanentemente actualizadas tanto funcional como tecnológicamente y enriqueciéndolas y mejorándolas. (Advice Consultancy Services, 2015)

3.1.2 Visión

Convertirse en el menor tiempo posible en una compañía de alta tecnología que innova permanentemente en la creación de nuevos esquemas empresariales orientados a preparar, incentivar y potenciar el talento y capacidades de nuestros Colaboradores para que de esta forma puedan crear y mejorar nuestros productos y servicios creando un circulo virtuoso cuyo fin último es el mejoramiento de la calidad de vida de todos los empleados. (Advice Consultancy Services, 2015)

3.1.3 Características deseables de los profesionales de Soft Warehouse S.A.

- Proponer ideas, soluciones y mejoras dentro de los lineamientos básicos que puedan ser de beneficio para los productos y/o la Compañía y/o sus Clientes.
- Hacer y colaborar con todo entusiasmo lo que la Compañía determine o decida a pesar de que no se esté 100% de acuerdo con ese camino o decisión.
- Hablar siempre bien de la Compañía y de sus productos.

3.1.4 Que es lo que no puede hacer un profesional de Soft Warehouse S.A.

- Desmotivar a los compañeros.
- Estigmatizar productos, metodologías, acciones, políticas o decisiones de la Compañía.

- Cualquier crítica que no sea constructiva.
- Revelar características, técnicas, diseños, ideas, problemas y cualquier información sobre clientes y prospectos a terceros y peor a la competencia.
- Ocultar o no informar de situaciones, comentarios, acciones que puedan: ya sea causarle un problema a la Compañía o ser una oportunidad de negocio.

3.1.3 Valores

- Calidad: La satisfacción del clientes es la mayor prioridad para ello se ejecuta el trabajo con un alto grado de calidad. Ofreciendo la máxima calidad en todo lo que se desarrolla ya que es la base fundamental de las acciones y surge de la pasión y orgullo.
- Honestidad: Las acciones se rigen por la verdad, honestidad y total transparencia. Se respetan los derechos y bienes de las personas.
- Innovación: La innovación está presente en todas las actividades de creación y mejora de los productos, procesos y actividades de gestión. Se busca constantemente alcanzar cambios significativos que generen valor para los clientes.
- Trabajo en equipo: Promover un ambiente de cooperación, constante entre el esfuerzo, integrando la comunicación y participación de los equipos de trabajo con las diferentes áreas de la compañía a fin de obtener los objetivos deseados.

3.1.4 Productos

FITBANK: es un Core Financiero integrado de última tecnología para automatización de la gestión financiera, de Bancos Comerciales y de Desarrollo orientado especialmente a controlar y mejorar la rentabilidad del negocio, elevar el nivel de servicio al cliente y facilitar el lanzamiento de nuevos productos.

En la Figura 7, se muestran la estructura de FITBANK la cual fue construida en un esquema de capas. La capa exterior pertenece al UCI (Universal Channel Interface) que permite la interacción con los clientes y otras aplicaciones, además posee una capa para el manejo de usuarios, roles, claves. La particularidad es que está orientado a bancos.

La capa intermedia es sumamente importante puesto que está conformada por una serie de módulos que son accesados mediante el uso de transacciones y a su vez alimentan la contabilidad, mediante esta concepción permite la adaptación de nuevos subsistemas. La

siguiente capa maneja la información de clientes y contabilidad, la información está organizado mediante niveles lo cual resulta sencilla la parametrización dependiendo del producto. Por parte del subsistema contable ha sido diseñado independientemente de cualquier plan preestablecido de cuentas y principalmente como un sistema gerencial orientado a proporcionar información financiera oportuna para el manejo del negocio financiero. En la parte superior izquierda se muestra el FIT SWITCH el cual está orientado al campo del dinero electrónico y ventanilla compartida, basada en la ISO 8583 (Estándar para Transacciones Financieras con Mensajes originados en una tarjetas), y en la ISO 20022 el cual permite al sector financiero contar con una plataforma común para el intercambio de datos electrónicos entre instituciones financieras.

Finalmente la última capa pertenece al módulo de información general (MIS) y un CRM con el fin de que la gerencia de la compañía cuente con toda la información y pueda realizar análisis de riesgos, rentabilidad entre otros.

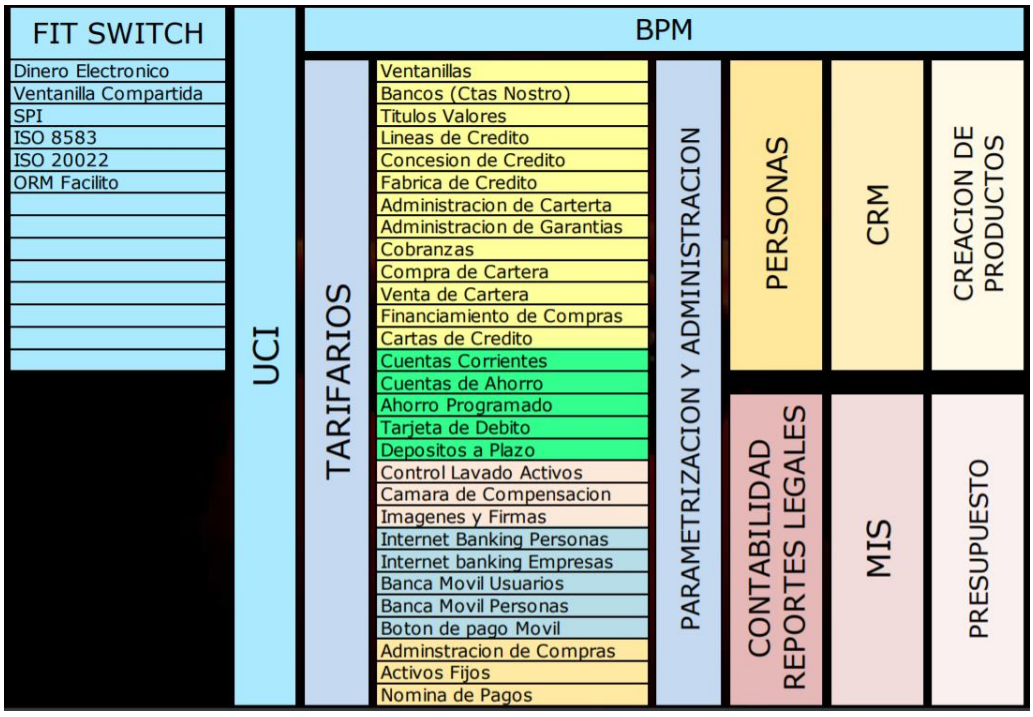

Figura 7. Módulos del producto FITBANK.
Elaborado por: (Advice Consultancy Services, 2015)

FITCOOP: es un Core Financiero integrado de última tecnología para automatización de la gestión financiera, de Cooperativas de Ahorro y Crédito de acuerdo a los

requerimientos de la SEPS[8] que está encargado de mejorar la rentabilidad y aumentar el servicio y la calidad de atención a los clientes del negocio.

En la Figura 8, se muestran la estructura de FITCOOP la cual fue construida en un esquema de capas. La capa exterior pertenece al UCI (Universal Channel Interface) que permite la interacción con los clientes y otras aplicaciones, además posee una capa para el manejo de usuarios, roles, claves. La particularidad es que está orientado a cooperativas es por eso que no posee un número mayor de subsistemas como lo posee FITBANK, se mantiene el mismo funcionamiento.

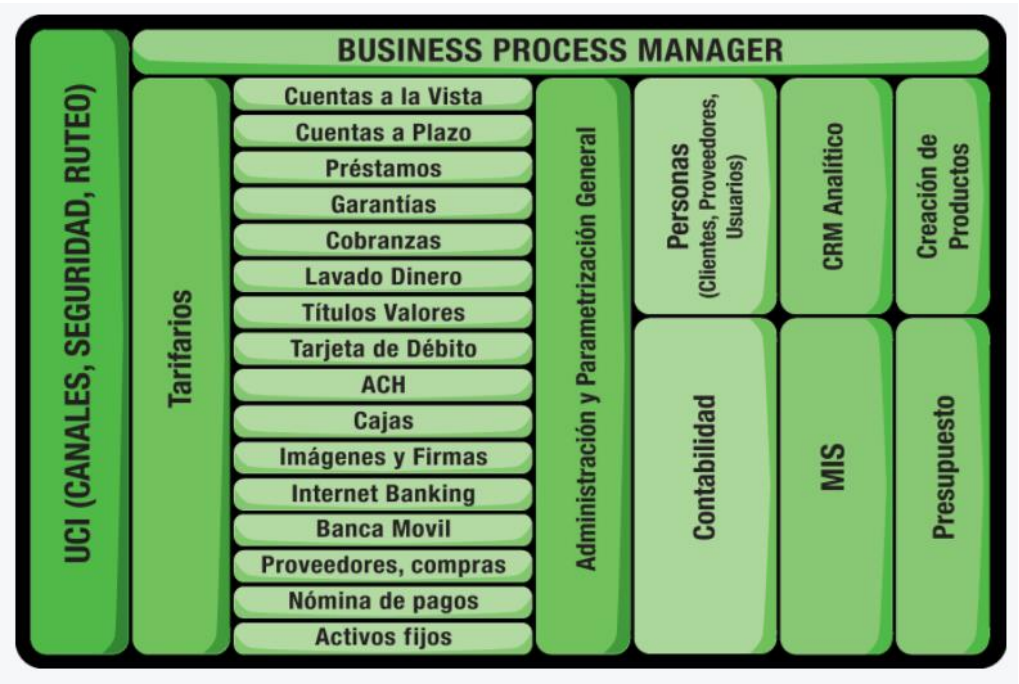

Figura 8.Módulos del producto FITCOOP.
Elaborado por: (Soft Warehouse, 2017)

FITFENICIOS: es un ERP[9] Financiero Administrativo integrado de última tecnología para automatización de la gestión administrativa y financiera de Empresas Comerciales e Industriales orientado especialmente a controlar y mejorar la rentabilidad del negocio y elevar el nivel de servicio al cliente.

[8] SEPS: Superintendencia de Economía Popular y Solidaria del Ecuador. Definición tomada de: http://www.seps.gob.ec/
[9] ERP: es un conjunto de sistemas que permiten la integración de ciertas operaciones empresariales, como la producción, logística, contabilidad, etc. Definición tomada de: http://www.aner.com/que-es-un-erp.html

De acuerdo a la Figura 9, se muestran la estructura de FITFENICIOS la cual fue construida en un esquema de capas. La capa exterior pertenece al UCI (Universal Channel Interface) que permite la interacción con los clientes y otras aplicaciones, además posee una capa para el manejo de usuarios, roles, claves. La capa intermedia es sumamente importante puesto que está conformada por una serie de módulos que son accedidos mediante el uso de transacciones y a su vez alimentan la contabilidad. Los subsistemas son aquellos que comparten un módulo de administración y parametrización general del sistema al igual que el manejo de tarifarios. La siguiente capa hacia adentro es la que capta la información sobre las personas y la contabilidad lo cual pertenecen a toda la estructura del cliente; el subsistema contable fue diseñado independientemente de cualquier plan preestablecido de cuentas y principalmente como un sistema gerencial orientado a proporcionar información financiera oportuna para el manejo del negocio.

Finalmente la última capa pertenece al módulo de información general (MIS) y un CRM analítico con el fin de que la gerencia de la compañía cuente con toda la información y pueda realizar análisis de riesgos, rentabilidad entre otros.

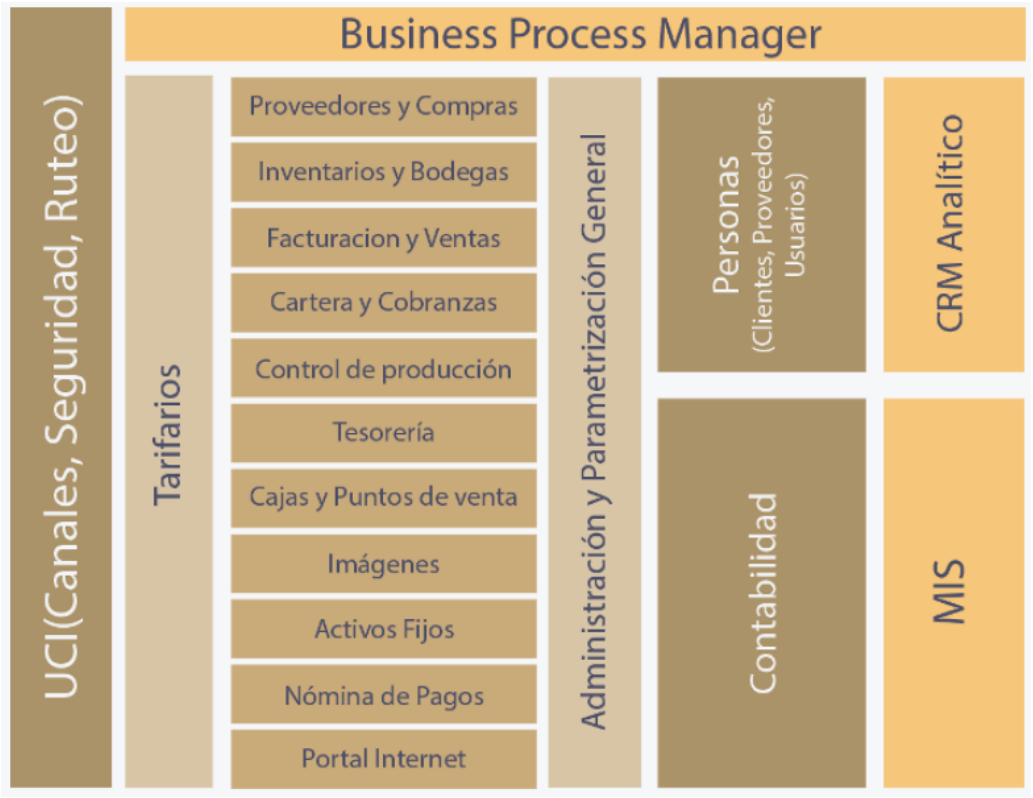

Figura 9. Módulos del producto FITFENICIOS.
Elaborado por: (Soft Warehouse, 2017)

3.2 Roles y responsabilidades del personal de seguridad de la información.

Actualmente Soft Warehouse S.A. no cuenta con un organigrama de seguridad de la informacion puesto que se maneja de forma lineal, pero a pesar de ello se cuenta con encargados de seguridad de la informacion en las distintas áreas. De acuerdo a las entrevistas realizadas se pudo denotar que el Ing. Heccer Benavides es el responsable del control de accesos a los ambientes de produccion y aplicativo, Ing.Galo Sánchez es el lider de proyecto y responsable de la distribucion de tareas al personal, el Ing. Hugo Zumarraga es el responsable de los accesos a la base de datos y réplicas, además dentro del área administrativa la Lic. Paola Freire es la responsable de la supervision de la informacion referente a la contabilidad que se maneja dentro de Soft Warehouse S.A.

3.3 Situación actual de la organización

Para poder conocer la situación actual de Soft Warehouse S.A se realizaron entrevistas al personal, consultas, revisión de documentación existente, observación y experiencia propia dentro del entorno empresarial durante un período de 3 años de trabajo en la compañía.

Las directrices que se tomaron en cuenta para analizar la situación actual en materia de seguridad de la información fueron tomados de la norma ISO/IEC 27002:2013 para Gestión de la Seguridad de la Información y en el Esquema Gubernamental de Seguridad de la Información (EGSI), que está dirigida a las Instituciones de la Administración Pública Central, Dependiente e Institucional del Ecuador.

Dominio de políticas de seguridad de la información

El dominio de políticas de seguridad de la información resalta que es importante contar con un documento de políticas de seguridad de la información que debe ser revisado anualmente o cuando se realicen cambios significativos a nivel operativo, legal, tecnológico, económico.

Soft WareHouse S.A. dispone de un documento de Gestión de Seguridad de la Información realizado en Noviembre de 2014 con versión 1.1, elaborado por Ardany Montúfar que no fue concluido y el estado en el que se encuentra es de un manual de Seguridad de Información preliminar, solo se toman en cuenta aspecto de forma general.

El documento posee un alcance de la gestión de seguridad de la información que contiene los siguientes temas con una definición, mas no se estipulan los procedimientos a seguir:

- Procedimientos y responsabilidades operacionales.
- Procedimientos para los proveedores de servicio.
- Procedimiento de administración de capacidad y aceptación de los sistemas.
- Procedimiento para proteger el software contra código malicioso.
- Procedimiento de administración de respaldos.
- Procedimiento para la administración de seguridad de redes.
- Procedimiento para manipulación de medios.
- Procedimiento de intercambio de información.
- Mecanismos de monitoreo de la infraestructura.
- Mecanismos de control de acceso a los sistemas de información.
- Requerimientos de seguridad de la información.
- Procedimientos y estándares de seguridad física.
- Administración de la continuidad.
- Procedimientos para la administración de riesgos.

Dominio de organización de la seguridad de la información

El dominio de organización de la seguridad de la información es muy importantes porque aquí se conforma el Comité de Gestión de Seguridad de la Información de la Institución (CSI) y se designan los integrantes que serán los responsables de la puesta en marcha de las normas que se estipularán en el documento de gestión de la seguridad de la información y las distintas funciones que debe mantener la coordinación de la gestión de seguridad de la información la cual debe realizar una asignación de responsabilidades sobre el oficial de seguridad de la información y el responsable de seguridad del área de tecnología de la información.

La compañía Soft WareHouse S.A. mantuvo en el año 2014 una estructura comité de seguridad de la información que se muestra en la Figura 10, que está liderado por la Gerencia General con sede en Quito que controla a tres ramas repartidas en Ambato, Cuenca y Quito; cada una de las sedes está controlada por un responsable de seguridad de la información (RSI).

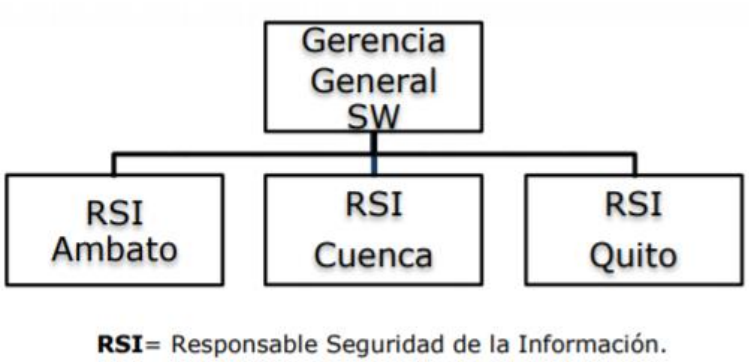

Figura 10. Estructura Comité Seguridad de la Información.
Elaborado por: (Advice Consultancy Services, 2015)

Dentro del esquema realizado no se detalla el nombre de las personas que serán responsables de la seguridad de la información en cada una de las sedes por lo tanto tampoco se estipulan las responsabilidades de cada uno de ellos.

Dentro la directriz de organización de la seguridad de la información se deben realizar acuerdos de confidencialidad y de no divulgación de la información.

La compañía gestiona los acuerdos de confidencialidad en el contrato de trabajo donde se detalla en el apartado Sexto que el trabajador se compromete a respetar los secretos empresariales sobre productos y administración, así como a guardar reserva sobre los clientes del empleador y la información que de éstos reciba por motivo de la realización de sus labores. Toda información considerada como confidencial por la empresa, no podrá ser usada por el trabajador en beneficio personal ni de terceros, ni en el presente ni en el futuro, sino exclusivamente en beneficio de la empresa empleadora y sus clientes. La infracción al compromiso de confidencialidad podrá ser juzgada bajo los artículos 284, 285 y 286 de la ley de Propiedad Intelectual del Ecuador.

Hay que destacar que la compañía maneja las consideraciones de seguridad cuando se trata con ciudadanos o clientes estableciendo criterios en base a derechos de propiedad intelectual y la protección de cualquier trabajo colaborativo dentro del contrato de trabajo estipulando que el trabajador mantendrá absoluta reserva y confidencialidad, durante y después de la relación laboral sobre tales inventos, patentes, desarrollos totales o parciales de programas y sus mejoras.

Pasando al ámbito de los acuerdos con terceras partes que es uno de los puntos que contempla la directriz de la organización en seguridad de la inflación, la compañía

mantiene un acuerdo con Level 3[10] que consiste en el hospedaje (Housing) de servidores propios de Soft Warehouse S.A., dentro del contrato se estableció un acuerdo a nivel de servicios (SLA), en el que se estipulan los niveles de continuidad y aspectos de seguridad (acceso a servidores, seguridad física). Además se mantiene un contrato con Amazon donde se hospeda un servidor en el que se encuentran claves de seguridad y los niveles de continuidad dentro contrato.

También se cuenta con dos proveedores de servicios de internet (Claro y TvCable), ya que en el caso en el que uno de los proveedores falla, inmediatamente se procede a conectarse al otro proveedor de servicio para mantener el servicio de soporte activo.

Dominio de la gestión de activos

El dominio de la gestión de activos es una parte importante para la administración de los riesgos donde se debe tomar en cuenta el inventario de los activos primarios en formatos físicos y/o electrónicos, los activos de soporte de hardware, los activos de soporte de software, los activos de soporte de redes y los activos referentes a la estructura organizacional. Dentro de la compañía Soft WareHouse S.A. se pudo evidenciar que no cuenta con una norma o directriz que exija realizar un inventario de los activos de información, por el momento solo se mantiene un registro actualizado de los artículos de oficina. Por el lado de los manuales e instructivos referentes a instalaciones, guías de usuario y de mantenimiento, en algunos casos se encuentran desactualizados; en el presente año se están actualizando algunos manuales que contienen procesos tales como: gestión de revisiones y Help desk.

Por el lado de las fuentes en el área de FIT 1 cada empleado descarga las fuentes en su computador personal de un servidor dentro de la compañía y las maneja según el requerimiento del cliente, no se maneja un control de versiones. Cada uno de los requerimientos están albergados en un Help desk, donde el cliente puede incluir requerimientos que son asignados al personal de soporte.

En el área de FIT 3 las fuentes están localizadas en servidores de Amazon el cual almacena sistemas para gestión de fuentes, Rhodecode maneja fuentes en mercurial y Gitlab que maneja fuentes en Git también maneja servidor en la nube como Dreamhost el

[10] Level 3: es una compañía multinacional estadounidense de telecomunicaciones y proveedor de servicios de Internet. Definición tomada de: https://es.wikipedia.org/wiki/Level_3_Communications

cual es un servidor compartido que almacena el Mantis (mantis.fit-bank.com) sistema de tickets de desarrollo donde se registran los incidentes y requerimientos reportados por clientes, Wiki (wiki.fit-bank.com) es un prototipo de base del conocimiento, DNS del dominio fit-bank.com y la página de fit-bank.com

En el inventario de activos de soporte de hardware no se maneja un registro de los equipos fijos como computadores portátiles debido a que cada empleado trabaja con su propio ordenador. Por el lado de los periféricos y dispositivos de almacenamiento como discos duros que albergan los respaldos mes a mes de los clientes no están en un área protegida. En el área administrativa si se maneja un inventario de los artículos de oficina, periféricos de salida y periféricos de entrada que se operan a diario.

Los activos de soporte de hardware en mal estado o descompuestos se almacenan en una bodega dentro del edificio.

En el inventario de activos de soporte de software no se maneja un registro de los programas o sistemas operativos que se utilizan. Están guardados en cajones para el uso común de la empresa. En el soporte de redes no se maneja un inventario de redes sin embargo se mantiene un registro de los cables de comunicaciones, switchs, ruteadores entre otros, pero se manejan diagramas de la red de comunicaciones que se manejan en la oficina de Quito, Cuenca y Ambato.

En el inventario de activos referente a la estructura organizacional se maneja un control de nómina por parte del área de recursos humanos, almacenando nombres, apellidos, cédula, número telefónico principal, correo electrónico personal y dirección domiciliaria de cada uno de los empleados.

Cada uno de los activos expuestos a continuación no están a cargo de un responsable directo que administre la información con el objetivo de mantenerla actualizada, sino que cada uno de los empleados actualiza su información de acuerdo a sus necesidades.

Un tema importante que abarca la directriz de la gestión de activos es el uso de un correo electrónico institucional que es utilizado específicamente para fines laborales que sean de la compañía y como un medio de comunicación con los clientes para brindar soporte adecuado y a tiempo. Cada miembro de la empresa es responsable de la información que envíe usando el correo institucional.

Una falencia que se pudo denotar en el entorno empresarial de Soft WareHouse S.A. es que no se maneja un control de acceso y uso de la internet enfocado en redes sociales, mensajería instantánea – chats con terceras personas que no incluyen a los clientes con

los que se trabaja día a día, videos, y otros ya que no hay bloqueos ni restricciones de acceso.
Otra falencia que se pudo observar es que al momento de realizar un video-conferencia con el cliente de suma importancia, no se desarrolla en un sitio cerrado donde se pueda mantener la confidencialidad de la información que es expuesta, sino que se desarrolla en un sitio abierto.

Dominio de la seguridad de los recursos humanos

El dominio de la seguridad de los recursos humanos resalta que la incorporación de una persona a la empresa es sumamente importante, lo que implica un nuevo acceso a sistemas de información sensibles de la empresa, además se deben tomar las consideraciones necesarias cuando un empleado deja la empresa por distintos motivos, es por ello que se deberían realizar acciones preventivas para evitar riesgos que se derivan a un mal uso de la información.

Cuando la compañía realiza una selección para incluir una nueva persona al entorno empresarial, en primera instancia se efectúa una verificación de la información personal, antecedentes penales y la información suministrada en la hoja de vida.
Si la compañía decide escoger a una persona que cumpla con los requerimientos solicitados se procede a realizar una prueba de aptitudes para evidenciar su conocimiento en los diversos temas.
Una vez que se escoge el personal adecuado se establecen términos y condiciones laborales dentro del contrato de trabajo donde se estipula la el compromiso del trabajador para prestar sus servicios de manera lícita a la compañía, a obedecer las órdenes impartidas por el empleador o superior inmediato, la duración del contrato contemplando un período de prueba de 90 días conforme lo establecido por el Código de Trabajo, se acuerda la remuneración mensual, la jornadas de trabajo, los acuerdo de confidencialidad y no divulgación, derechos de propiedad intelectual, compromisos, derechos y responsabilidades que debe cumplir el trabajador como el empleador.
Una vez definidas las funciones y responsabilidades de cada persona, durante el contrato, se otorga un rol dentro del sistema con sus respectivos accesos, permitiéndoles acceder a la información de acuerdo a lo que necesita de manera informal.

Cuando se termina un contrato laboral, la persona en cuestión debe anticiparse a su renuncia o despido con un lapso de quince días para poder distribuir las funciones que estuvo realizando y empezar un proceso de traspaso de conocimientos a otro empleado, se procede a archivar en carpetas la información como cédula, currículo, documentos médicos entre otros por el lado del correo institucional, claves de acceso al sistema son retirados y suspendidos para evitar cualquier percance.

Dominio de la seguridad física y del entorno

El dominio de la seguridad física y del entorno se ocupa de evitar el acceso físico no autorizado, y el daño a las instalaciones.

La compañía Soft Warehouse S.A. está conformada por dos oficinas en la ciudad de Quito.

Ofician FIT 1: conformada por una sala de reuniones amplia y el área de soporte de FIT 1 que está a cargo de cooperativas de ahorro pequeñas.

Oficina FIT 3: conformada por el área de gerencia general, área de recursos humanos y el área de soporte de FIT 3 que está a cargo de bancos y cooperativas de ahorro grandes.

Las dos oficinas están unidas por un área de recepción dirigida por una persona encargada de la administración y del apoyo en la oficina, es el primer contacto empresarial cuya responsabilidad principal es recibir a los clientes solicitando su nombre para poder anunciarlos de manera adecuada; además de responder, registrar y devolver llamadas telefónicas que son re-direccionadas al personal de soporte de la compañía.

Cada una de las oficinas maneja un sistema de alarmas contra incendios, un extintor ubicado en un lugar estratégico y un sistema de vigilancia que está a cargo de los guardias de seguridad del edificio ayudados por dos cámaras de seguridad en cada una de las puertas de acceso a cada una de las oficinas. Lo que se pudo observar dentro del entorno empresarial es que no se maneja un control de protección de equipos (servidores) ante daños provocados por temperatura y humedad. Lo que se puede enfatizar es que el mantenimiento que se presta a equipos de oficina como impresoras y computadoras que son usadas por la secretaria y contadora.

Un punto clave que se debe tomar en cuenta dentro del control de acceso físico y del entorno que maneja la compañía es el uso de un reloj biométrico para la entrada y salida del personal con el fin de respetar la hora de llegada y salida, pero si es persona externa se procede a tomar los datos antes de ingresar.

Dominio de la gestión de comunicaciones y operaciones

El dominio de la gestión de comunicaciones y operaciones tiene como objetivo fundamental el aseguramiento del funcionamiento de la operación correcta de los medios de procesamiento de la instalación donde se procesa la información, esto incluye el desarrollo de procedimientos de operación apropiados.

La compañía Soft Warehouse S.A. ha documentado manuales enfocados en el área técnica para el uso de software, manuales para el reinicio del sistema, manuales de los procesos de calidad y operativos, manuales de cada uno de los flujos de cada módulo con sus respectivas transacciones del sistema, manuales de usuario para cada uno de clientes con las respectivas indicaciones que se deben tener en cuenta para usar de forma correcta el sistema, y posibles problemas con su respectiva solución.

En algunos casos se debería realizar una actualización de la información de cada manual debido a los cambios que se van dando año tras año. Cuando se realiza un cambio esto depende de cada cliente, es decir, se realiza el cambio en el manual y se descarta la versión anterior solo para ese cliente, mas no se efectúa el cambio para todos los clientes. La compañía no documenta por medio de una gestión de cambios las actualizaciones que se van realizando, y es hace muy difícil saber cuáles son las correcciones anteriores.

Para mantener las operaciones controladas, evitando modificaciones no autorizadas o no intencionales, todas las funciones de Soft Warehouse S.A. son definidas y generalmente están asociadas a un rol operativo, este rol es empleado por el personal a lo largo de su interacción con los sistemas limitando sus interacciones con el mismo con el fin de solamente permitir modificaciones acorde a su función.

Adicionalmente este control extiende a ambientes y entornos: desarrollo, pruebas, soporte y producción; cada ambiente está aislado uno de otro y se tienen controles de acceso a los mismos con el fin de que se mantenga la integridad de información y no se afecte la operación de los clientes, los accesos a estos ambientes es protegido con medidas de autenticación y los accesos son otorgados acorde las funciones que cumple el recurso.

En algunos casos los ambientes se encuentran hospedados fuera de Soft Warehouse S.A., están resguardados en Level 3, donde se paga por Housing de dichos servidores. Para permitir un nivel alto de operaciones y comunicaciones de los clientes e interno se tiene un contrato de nivel de servicio (SLA) con Level 3 donde se estipula un “up-time”

superior al 99%. Además en el contrato se estipuló mediante políticas de seguridad que el acceso a los servidores únicamente se realizará mediante una cita formal entre Soft Warehouse S.A. y Level 3, todo cambio de hardware o software a los servidores lo realizará el personal de Soft Warehouse S.A. en ningún caso lo podrá hacer directamente un encargado de Level 3.

Para prevenir y atender a la brevedad posible incidentes se cuenta con servicios que miden la carga en transacciones generadas y servicios de notificación de errores de conexión con internet o en entre módulos del sistemas estas medidas permiten determinar cuellos de botella y fallas en el sistema de forma relativamente rápida con la finalidad de resolverlos a la brevedad posible.

Dominio de control de acceso

El dominio de control de acceso tiene como objetivo fundamental controlar en base a restricciones y excepciones el ingreso a la información confidencial de la empresa por medio de procedimientos, asignaciones de derechos de accesos entre otros.

La compañía Soft Warehouse S.A. maneja un control de accesos controlado, si una persona desea realizar consultas a una base de datos requerida se debe pedir una autorización de formato físico y digital el cual contiene el motivo por el cual desea acceder, las tablas que va a utilizar y se procede a asignar un usuario y contraseña para el acceso. Lo mismo ocurre en el caso de acceso a los servidores de la compañía.

Dominio de la gestión de incidentes

El dominio de la gestión de incidentes de la seguridad de la información tiene como objetivo principal de esta directriz es garantizar una correcta gestión de los incidentes de seguridad aplicando un proceso de mejora continua con el fin de monitorear los incidentes de seguridad de la información en el entorno empresarial.

La compañía Soft Warehouse S.A. no mantiene una bitácora de incidentes donde se pueda reportar el día, fecha, hora del problema, área afectada, cual fue el impacto que causó al sistema y como se resolvió el problema; se pudo notar que no existe un responsable directo de gestionar los incidentes de seguridad de la información.

Actualmente el personal no tiene un amplio conocimiento en cómo actuar ante un incidente de seguridad, puesto que no se tienen bien definidos los planes de contingencia para solventar este problema, únicamente se tienen planes de contingencia cuando se

suscitan problemas con el sistema inmediatamente se procede a levantar un servidor de réplica de modo lectura a modo escritura para que la cooperativa o banco siga con sus labores normales.

Es muy importante recolectar la evidencia para asegurar el cumplimiento de los requisitos legales, la compañía no recolecta evidencia de los incidentes de seguridad únicamente la monitorización del sistema cuando sufrió un altercado de funcionamiento otorgado por Level 3.

Dominio de gestión de la continuidad del negocio

El dominio de gestión de la continuidad del negocio es una parte principal que influye en la continuidad del negocio y los procesos que conforman la organización. El objetivo fundamental de la continuidad es estar preparados y reaccionar a la interrupción de las actividades del negocio y proteger los procesos más importantes de la compañía ante los desastres o fallos de los sistemas de información.

La compañía Soft Warehouse S.A. no tiene un responsable directo encargado de la continuidad de los servicios informáticos en el área de tecnologías de la información puesto que maneja un organigrama lineal. Además carece de un mapa de riesgos que permite identificar las amenazas sobre los activos con el fin de priorizar aquellos problemas que pueden provocar una paralización del sistema.

Hay que resaltar que la compañía si maneja estrategias asociadas a un plan de continuidad como son: Manejo óptimo de respaldos mes a mes de las cooperativas y bancos, reinicio del sistema cuando el cliente lo solicite, servidores de réplica, seguro para los activos de la compañía y procedimientos para la recuperación del servicio.

4. Capítulo: Desarrollo de la Propuesta de Políticas de Seguridad de la Información.

En el presente capítulo se detallará cada uno de los dominios, listados en la ISO 27002 y su equivalente en el EGSI, dentro de cada dominio existen objetivos de control con sus respectivos controles; en la Propuesta de Políticas de Seguridad de la Información no se detallan todos los controles sino que se acogieron los que mejor se aplicaban a Soft Warehouse S.A.

4.1 Justificación

El desarrollo de esta disertación se fundamenta en una propuesta de políticas de seguridad de la información que pueda ser implementada en el entorno empresarial de Soft Warehouse S.A., puesto que es una compañía que constantemente está manejando información importante y posee una amplia nómina de empleados encargados en dar soporte a cada uno de los clientes, por lo cual aplicar políticas de seguridad de la información beneficiaria al personal de una herramienta que pueda facilitar la toma de decisiones correcta para poder protegerse de una forma apropiada ante amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la compañía. La seguridad de la información actualmente se ha convertido en una de las preocupaciones más críticas en todo tipo de organizaciones; cada concepto que se tomó en cuenta dentro del desarrollo de esta investigación tiene como objetivo brindar a la compañía un conjunto de buenas prácticas para poder crear una cultura de seguridad.

4.2 Motivación

Los motivos principales para desarrollar esta propuesta fueron:

- El interés de la Gerencia General en fortalecer a la compañía en temas de seguridad de la información con el fin de crear una cultura de seguridad dentro del ambiente laboral y de esta forma orientar a cada uno de los empleados de Soft Warehouse S.A. en el manejo de buenas prácticas a la hora de desempeñar su trabajo.
- La preocupación de la Gerencia General en resguardar su información frente a personas no autorizadas que puedan atentar contra la integridad de la compañía.
- El interés de la Gerencia General en cumplir con medidas de seguridad de información a proveedores de software para cooperativas del Ecuador dispuestas por la SEPS (Superintendencia de Economía Popular y Solidaria).

- La preocupación de la Gerencia General en controlar la asignación de derechos de acceso a los ambientes, sistemas de información, bases de datos y servicios de información.
- La aspiración de la Gerencia General en conocer y llevar un inventario de activos de forma ordenada para realizar una buena administración de los riesgos.

4.3 Indicaciones

Dentro de esta sección se proporcionará información que puede ser necesaria considerar para poder alcanzar el objetivo de control de cada dominio de la ISO 27002 que fue tomado en cuenta para la propuesta de políticas se seguridad de la información para la compañía Soft Warehouse S.A.

4.3.1 Dominio 1: Políticas de seguridad de la información

Es recomendable crear políticas para la seguridad de la información de la organización, con el apoyo de la gerencia general y la difusión a todo el personal y terceros a la misma. Este documento va a variar de acuerdo a la organización que lo requiera al igual que se suelen utilizar distintos términos para referirse al documento tales como estándares, directivas o reglas.

Las políticas de seguridad de la información deben respetarse dentro de la compañía pero si se distribuyen fuera de la misma, se debe tener cuidado de no divulgar información confidencial que puede atentar contra la integridad de la compañía.

De acuerdo con el control de la revisión de la política de seguridad se debe tener el consentimiento del área administrativa de la compañía para obtener la aprobación de la misma.

4.3.2 Dominio 2: Organización de la seguridad de la información

De acuerdo con el control de la asignación de responsabilidades para la seguridad de la información en la mayoría de las organizaciones nombran a un Oficial de Seguridad de la Información el cual será el responsable general del desarrollo e implementación de la

seguridad de la información y colaborará con la identificación de controles óptimos para aplicarlos dentro del entorno empresarial.

De acuerdo con el control de contacto con las autoridades puede ser un requisito para respaldar la gestión de los incidentes de seguridad de la información o el proceso de continuidad y los planes de contingencia. Los contactos con otras autoridades incluyen los servicios públicos, servicios de emergencia, proveedores de internet, electricidad, salud y seguridad además se puede establecer acuerdos de intercambio de información entre los recursos de la compañía para mejorar la seguridad por medio de grupos de interés especial.

De acuerdo con el control de dispositivos móviles hay que tener en cuenta que las conexiones inalámbricas son similares a otros tipos de conexión de red por lo tanto algunos protocolos de seguridad inalámbrico son débiles y la información almacenada en los dispositivos móviles puede no estar respaldada debido al ancho de banda limitado ya que al realizar una copia de seguridad puede que no esté conectado a la red.

4.3.3 Dominio 3: Seguridad de los recursos humanos

De acuerdo con el control de la investigación de antecedentes antes de la contratación es importante que la verificación de antecedentes de todos los candidatos se lo realice de conformidad con las leyes y reglamentos del estado.

Con referencia a lo anterior la organización debe asegurar que los candidatos acepten los términos y condiciones de contratación.

De acuerdo con el control de las responsabilidades de gestión durante el empleo si el empleado no conoce sus responsabilidades puede causar daños considerables a la compañía, es por eso que si se mantiene al personal motivado es probable que sea más confiable y cause menos incidentes de seguridad de la información. Hay que considerar que por medio de un código de conducta se puede establecer las responsabilidades de seguridad de la información del empleado con relación a la confidencialidad, protección de datos, ética, uso apropiado de los equipos de la compañía e instalaciones, así como las prácticas que realice dentro de la misma.

Es evidente entonces que una mala gestión puede ocasionar que el personal se sienta infravalorado, lo que desemboca en un control de la seguridad de la información negativa y un gran impacto a la compañía. Es por ello que al diseñar programas de concientización es importante no solo tomar en cuenta el "qué" y el "cómo" sino también el "por qué" de las cosas. Es sumamente importante que los empleados conozcan el objetivo que tiene la seguridad de la información y el impacto tan grande en la compañía por medio de su comportamiento.

El control de la concienciación, formación y capacitación en seguridad de la información seguridad puede llevarse a cabo con la colaboración de otras actividades como por ejemplo una capacitación general de TI o de seguridad en general.

El control del proceso disciplinario puede convertirse en una motivación e incentivo si se definen sanciones positivas por un comportamiento intachable con respecto a la seguridad de la información.

4.3.4 Dominio 4: Gestión de activos.

De acuerdo con control de inventario de activos este debe ser preciso, actualizado, consistente y alineado con los otros. Se sugiere utilizar el esquema que provee la ISO 27005 acerca de la división de inventarios para obtener una idea más clara de que activos considerar.

De acuerdo con el control de propiedad de activos se debe designar un responsable encargado de controlar todo el ciclo de vida del mismo, pero eso no significa que tiene el derecho de propiedad sobre ese activo.

De acuerdo el control de la clasificación de la información sirve de ayuda a que las personas responsables sepan cómo manejarla y protegerla. Al crear grupos de información con necesidades de protección similares e información específica ayuda a que los procedimientos de seguridad se faciliten puesto que este enfoque reduce la necesidad de ir evaluando uno por uno. Hay que tener en cuenta que la información puede dejar su estatus de sensible o critica después de un cierto período de tiempo, es decir, cuando la información se ha hecho pública; hay que tener muy en cuenta ya que esto puede llevar a la generación de controles innecesarios y a gastos adicionales.

De acuerdo con el control de etiquetado de información se considera un requisito para los acuerdos de intercambio de información, pero en algunas ocasiones tienen efectos negativos ya que los activos clasificados son más fáciles de identificar y consecuentemente robar por personas internas o por atacantes. El uso de etiquetado físico es una forma común de identificación.

De acuerdo con el control de eliminación de activos se debe verificar que los dispositivos dañados que contienen datos confidenciales puede requerir una evaluación de riesgos para determinar si el activo debe destruirse físicamente en lugar de raparlo o desecharlo.

4.3.5 Dominio 5: Control de accesos

De acuerdo con el control de accesos basado en roles es un enfoque utilizado con éxito por muchas organizaciones para vincular los derechos de acceso con roles de negocios.
Existen dos principios básicos que dirigen el control de accesos como son:

- La necesidad de saber: solo se le concede acceso a la información que necesita para realizar sus tareas.
- La necesidad de uso: solo se le concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, salas) que necesita para realizar su tarea.

De acuerdo con el control de acceso a redes y servicios asociados se debe tener en cuenta que las conexiones de procedencias inseguras pueden afectar a la organización. Se debe tomar en cuenta la creación de controles de conexión a la red o lugares de alto peligro de robo de información.

De acuerdo con el control de la gestión de los derechos de acceso con privilegios especiales se debe considerar que el mal uso de los privilegios otorgados como administrador puede afectar los controles del sistema o del ambiente donde se está trabajando.

De acuerdo con el control de uso de información confidencial para la autenticación la provisión de inicio de sesión único (SSO) u otras herramientas de administración de información de autenticación reduce la cantidad de información de autenticación secreta que los usuarios deben proteger y, por lo tanto, puede aumentar la efectividad de este

control. Sin embargo, estas herramientas también pueden aumentar el impacto de la divulgación de secretos información de autenticación.

4.3.6 Dominio 6: Criptografía

De acuerdo con el uso de controles criptográficos es necesaria una política sobre el uso de los mismos para maximizar los beneficios y minimizar los riesgos de atentar con la disponibilidad, confidencialidad e integridad de la información de la organización.

Tomar una decisión sobre si una solución criptográfica es apropiada debe verse como parte de la de evaluación de riesgos y selección de controles. Se realiza este seguimiento para analizar si un control criptográfico es apropiado, qué tipo de control se debe aplicar y para qué propósito y procesos de negocios. Se debe buscar asesoramiento especializado para seleccionar los controles criptográficos apropiados para cumplir objetivos de la política de seguridad de la información.

4.3.7 Dominio 7: Seguridad física y ambiental

De acuerdo con el control de seguridad física y ambiental, la aplicación de controles físicos, especialmente para las áreas seguras, debe adaptarse a la técnica y las circunstancias económicas de la organización. Un área segura puede ser una oficina con cerradura o una sala con una barrera de seguridad, en el caso de organizaciones grandes es posible que se necesiten barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad.

De acuerdo con el control de protección contra amenazas externas y ambientales se debe obtener asesoramiento especializado por parte de los organismos del Estado para sobrellevar los incidentes en caso de desastres naturales y acciones dañinas generadas por el hombre.

De acuerdo con el control de seguridad de los equipos y activos fuera de las instalaciones resalta que los riesgos, por ejemplo, de daños, robo pueden variar considerablemente de un lugar a otro y se debe tener en cuenta al determinar los controles más apropiados.

4.3.8 Dominio 8: Seguridad de operaciones

De acuerdo con el control de gestión del cambio es conveniente que deban existir responsabilidades y procedimientos formales de gestión con el fin de garantizar un control satisfactorio de los cambios. Cuando exista un cambio se debe conservar un registro de auditoria que contenga toda la información relevante. El control inadecuado de los cambios en las instalaciones y sistemas de procesamiento de información es una causa común para que existan fallas de seguridad.

De acuerdo con el control de separación de entornos de desarrollo, pruebas, producción y capacitación se puede denotar que las actividades de desarrollo y pruebas pueden causar problemas graves como por ejemplo, modificaciones no deseadas en archivos, ambientes, scripts; así que es necesario mantener un entorno conocido y estable en el que se puedan realizar pruebas y evitar el acceso inadecuado del desarrollador al entorno de producción. Al separar los ambientes de desarrollo, pruebas y producción se reduce el riesgo de cambios accidentales o el acceso no autorizado al software y datos confidenciales.

De acuerdo con el control de protección contra el código malicioso hay que tener en cuenta que el uso de software de detección y reparación de malware solo como un control no suele ser adecuado y comúnmente debe ir acompañado de procedimientos operativos que impidan la introducción de código malicioso.

De acuerdo con el control de la protección del registro de información hay que tener en cuenta que los registros del sistema a menudo contienen un gran volumen de información por lo cual si los datos pueden ser modificados o eliminados esto va a causar una falsa sensación de seguridad es por ello que realizar una copia de registros en tiempo real a un sistema fuera del control de un administrador u operador se puede utilizar para salvaguardar los registros.

De acuerdo con el control de sincronización de relojes es importante porque garantiza la exactitud de los registros obtenidos y estos pueden ser utilizados para investigaciones o como evidencia en casos legales.

De acuerdo al control de gestión de vulnerabilidades técnicas el mantener un inventario actual y completo de activos es un requisito previo para que el manejo de vulnerabilidades sea más óptimo. Es conveniente que se tomen medidas apropiadas y oportunas en respuesta a las vulnerabilidades más graves para se debe establecer un proceso de gestión

efectiva en donde: la organización debe definir y establecer las funciones y responsabilidades asociadas a la gestión de vulnerabilidades, incluyendo la vigilancia y evaluación de las mismas además de un seguimiento de activos.

4.3.9 Dominio 9: Seguridad de las comunicaciones

De acuerdo con el control del control de seguridad en los servicios de red es importante recalcar que estos incluyen la provisión de conexiones, servicios de red privada, soluciones de seguridad de redes administradas, como firewalls y sistemas de detección de intrusos.

La seguridad de los servicios de red son: un conjunto de herramientas (Software y Hardware) diseñados para aplicar medidas de cifrado y control de accesos necesarios para la conexión segura con los servicios de red de conformidad con las reglas de seguridad y conexión de red.

De acuerdo con el control de segregación de redes éstas a menudo se extienden más allá de los límites de la organización, ya que requieren la interconexión o el intercambio de procesamiento de información. Tales extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que utilizan la red, algunos de los cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.

De en el control de acuerdos de intercambio de información éstos pueden ser electrónicos o manuales, y pueden tomar la forma de contratos formales.

Conforme al control de acuerdos de confidencialidad y secreto de éstos protegen la información de la organización e informan a los signatarios de su responsabilidad de proteger, usar y divulgar información de manera responsable y autorizada.

4.3.10 Dominio 10: Adquisición, desarrollo y mantenimiento de los sistemas de información

De acuerdo con el control de análisis y especificación de requisitos de seguridad de la información estos deben identificarse utilizando diversos métodos, como derivar requisitos de cumplimiento de políticas y regulaciones, modelos de amenazas, revisiones

de incidentes o uso de umbrales de vulnerabilidad. Los resultados de la identificación deben ser documentados y revisados por todas las partes interesadas.

De acuerdo con el control de la política de desarrollo seguro, las técnicas de programación deberían usarse tanto para nuevos desarrollos como en escenarios de reutilización de códigos donde los estándares aplicados al desarrollo pueden no conocerse o no ser consistentes con las buenas prácticas. Deben considerarse estándares de codificación segura y, cuando corresponda, su uso obligatorio.

De acuerdo con el control de procedimiento de control de cambios, se debe incluir una evaluación de riesgos, un análisis de los impactos de los cambios y las especificaciones de controles de seguridad necesarios. Este proceso también debe garantizar que los procedimientos de seguridad y control existentes no estén comprometidos, que los programadores de soporte solo tengan acceso a esas partes del sistema necesario para su trabajo y que se obtenga el acuerdo formal y la aprobación de cualquier cambio.

4.3.11 Dominio 11: Relaciones con proveedores

De acuerdo con el control de política de seguridad de la información con proveedores hay que tener en cuenta que la información puede ser puesta en riesgo por proveedores con una administración inadecuada de seguridad de la información. Se deben identificar controles para administrar el acceso de los proveedores a las instalaciones de procesamiento de información como por ejemplo, si existe una necesidad especial de confidencialidad de la información, los acuerdos de confidencialidad pueden ser usados.

De acuerdo con el control de tratamiento del riesgo dentro de acuerdos con proveedores hay que enfatizar que los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de proveedores. Por lo tanto, se debe tener cuidado de incluir todos los riesgos relevantes de seguridad de la información y requisitos. Los acuerdos de proveedores también pueden involucrar a otras partes (por ejemplo, subproveedores).

De acuerdo con el control de supervisión y revisión de los servicios prestados por terceros la responsabilidad de gestionar las relaciones con los proveedores debe asignarse a un individuo o equipo de administración de servicio. Además, la organización debe

garantizar que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos. La organización debe mantener un control general suficiente y visibilidad de todos los aspectos de seguridad para información sensible o crítica o instalaciones de procesamiento de información a las que se accede, procesa o gestiona.

4.3.12 Dominio 12: Gestión de incidentes en la seguridad de la información

De acuerdo con el control de notificación de los eventos de seguridad de la información todo el personal debe ser conscientes de su responsabilidad de informar los eventos de seguridad lo más rápido posible. También deben conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se debe acudir lo más pronto posible.

De acuerdo al control de aprendizaje de los incidentes de seguridad de la información se puede obtener un conocimiento especial de cómo resolver el problema con el fin de reducir el impacto de incidentes futuros. Este conocimiento puede estar incluido en una base de conocimiento y estar disponible para cada uno de los recursos de la compañía.

4.3.13 Dominio 13: Aspectos de seguridad de la información en la gestión de la continuidad del negocio

De acuerdo con el control de planificación de la continuidad de la seguridad de la información la compañía debe realizar un análisis de cómo se encuentran los procesos de continuidad del negocio y las medidas a tomar para gestionar los desastres.

De acuerdo al control de redundancias, la implementación de redundancias puede introducir riesgos a la integridad o confidencialidad de la información y sistemas de información, que deben tenerse en cuenta al diseñar sistemas de información.

4.3.14 Dominio 14: Continuidad

De acuerdo con el control de derechos de propiedad intelectual es importante tener en cuenta que incluyen copyright de software o documento, derechos de diseño, marcas comerciales, patentes y licencias de código fuente, la infracción de derecho de propiedad intelectual puede llevar a acciones legales que pueden implicar multas y procedimientos penales.

De acuerdo con el control de la protección de los registros de la compañía es necesario tener en cuenta que estos registros pueden ser retenidos de manera segura para cumplir con los requerimientos legales, reglamentarios así como apoyar en actividades comerciales necesarias. La ley o regulación nacional puede establecer el período de tiempo y el contenido de datos para retención de información.

5. Capítulo: Conclusiones y Recomendaciones

Conclusiones

1. Las organizaciones diariamente recopilan, procesan, almacenan y transmiten información de muchas formas, existe un sinnúmero de personas que usan esta información no solo considerándola como un escrito, números, nombres, direcciones, cuentas, sino como un activo valioso que merece y requiere protección contra cualquier incidente que atente contra la disponibilidad, continuidad e integridad de la misma.
2. La información que maneja Soft Warehouse S.A. es muy valiosa, y está sujeta a incidentes tanto internos como externos a la compañía, ya sea por la ausencia de controles clave, documentación no actualizada, cambio de personal, ausencia de una cultura de seguridad por parte del personal. Por lo tanto, dada la multitud de amenazas que atentan contra la compañía se procedió a realizar un manual de políticas de seguridad de la información que ayudarán a mitigar el riesgo contra amenazas, vulnerabilidades y reducir el impacto contra los activos.
3. El proceso de creación de las políticas de seguridad de la información se determinó que para que una compañía maneje niveles de seguridad aceptables debe seguir cada uno de los dominios y controles recomendados por la ISO/IEC 27002:2013 que brinda las mejores prácticas para hacer que la gestión de la seguridad de la información sea más fácil manejarla en todo tipo de empresas.
4. En cuanto a los dominios que una empresa debe contar como prioritarios son: Dominio 4: Gestión de Activos, Dominio 5: Control de Accesos, Dominio 12: Gestión de Incidentes de la Seguridad de la Información y el Dominio 13: Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.
5. En la investigación realizada para la creación de políticas de seguridad de la información se tomó en cuenta la ISO/IEC 27002:2013, estándar que brinda un conjunto de guías y buenas prácticas para manejar e implementar seguridad de la información en cualquier entorno empresarial. Y el EGSI (Esquema Gubernamental de Seguridad de la Información) emitido por la Secretaria Nacional de Administración Pública del Ecuador.

Recomendaciones

A lo largo del desarrollo de la propuesta de políticas de seguridad de la información enfocado al entorno empresarial de Soft Warehouse S.A. se obtuvieron los siguientes resultados.

1. Es importante tener el apoyo de la Gerencia General para la realización y ejecución de los proyectos relacionados con seguridad de la información con el fin de generar valor a la compañía; debido a que la falta de apoyo económico destinado a implementar medidas de seguridad, ocasiona que la compañía este expuesta a un sinnúmero de riesgos.
2. Para realizar una política de seguridad se recomienda priorizar procedimientos, mecanismos y activos en los que la organización presente problemas de seguridad, está priorización debe ejecutarse en base al impacto del problema con fin de solventar inconvenientes de mayor importancia.
3. Cada uno de los comportamientos individuales determinan la cultura de la compañía, si se provee de buenas prácticas que fomenten una cultura de seguridad de la mano de la concienciación y el apoyo de cada uno de los empleados se puede mitigar uno de los factores más importantes que atenta contra la seguridad de la información que es principalmente por personal interno, empleados y exempleados de las organización.
4. La realización de un inventario de activos facilita la designación de los responsables a cargo, permite mantener un control durante todo su ciclo de vida y evita posesiones indebidas que atenten contra la compañía.
5. Manejar un control de accesos apoyado en técnicas de autenticación y autorización proporciona mayor control en la conexión a los sistemas, base de datos, y sistemas de información; limitando el acceso y los privilegios sobre los sistemas.
6. La segregación de redes minimiza el nivel de acceso a la información sensible, de modo que se hace más difícil para el atacante localizar y acceder a la información.

Finalmente, en base al entorno empresarial de Soft Warehouse S.A. es importante ejecutar un plan de implementación que estará a cargo del Oficial de Seguridad de Información, quien será el responsable de controlar el cumplimiento de cada dominio expuesto en el

documento de políticas de seguridad de la información, el Responsable del Área de Tecnología contribuirá con ideas y soporte necesario en las disposiciones que determine el Oficial de Seguridad de la Información.

De primera instancia se debe realizar una priorización de Dominios, la cual se realiza en base a los objetivos de seguridad del negocio y las regulaciones vigentes; con esto se determina el nivel de importancia y urgencia que tiene cada Dominio para el negocio.

Se puede continuar por realizar una priorización de los Objetivos de Control de cada Dominio, basándose en la importancia e impacto que tiene dicho objetivo respecto a su correspondiente Dominio.

Por último se debe realizar una priorización de los Controles de acuerdo a su grado de rendimiento, importancia e influencia sobre el Objetivo de Control.

De esta manera se podrá crear una matriz de prioridad, que va a reflejar cada Dominio, Objetivos de Control y Controles seguido de un porcentaje de cumplimiento, de tal forma que para realizar un análisis del seguimiento, será más óptimo visualizar que Controles, Objetivos de Control o Dominios no se están cumpliendo y de esta forma tomar las medidas necesarias con el fin de lograr la implementación del Dominio.

Considerado la priorización de Dominios y el estado actual de la compañía, Soft WareHouse S.A. puede empezar por la implementación de los siguientes dominios:
Dominio 2: Organización de la Seguridad de la Información.
Dominio 4: Gestión de los Activos.
Dominio 5: Control de Accesos.

En un tiempo estimado de 3 dominios cada 3 meses, es decir que en un período de 15 meses, Soft WareHouse S.A. tendrá implementado el Proyecto de Seguridad de la Información basado en Políticas de Seguridad de la Información.

Bibliografía

27001Academy. (2017). Recuperado el 06 de Noviembre de 2017, de ¿Qué es norma ISO 27001? | 27001Academy: https://advisera.com/27001academy/es/que-es-iso-27001/

Advice Consultancy Services. (2015). *Identidad Corporativa "Soft Warehouse"*. Quito. Recuperado el 30 de Noviembre de 2017

Areitio, J. (2008). *Seguridad de la Informacón, Redes, Informatica y Sistemas de Información.* Madrid, España: Paraninfo S.A. Recuperado el 30 de Octubre de 2017, de https://books.google.com.ec/books?id=_z2GcBD3deYC&pg=PA46&lpg=PA46&dq=objetivos+de+la+politica+ambitos+de+la+politica+procedimientos+de+seguridad+a+adoptar&source=bl&ots=wshrwJHWUg&sig=H7RcAtKFxQExo0AkPiOmUBgX0mg&hl=es&sa=X&ved=0ahUKEwiXg6uGn5nXAhXCWCYKHU

Arma International. (26 de Enero de 2016). Recuperado el 31 de Octubre de 2017, de Encuesta: los empleados toman datos confidenciales cuando se van: http://www.arma.org/r1/news/newswire/2016/01/26/survey-employees-take-sensitive-data-when-they-leave

Arora, V. (2017). *Comparing different information security standards: COBIT vs ISO 27001*. Recuperado el 09 de Noviembre de 2017, de https://s3.amazonaws.com/academia.edu.documents/31868881/CPUCIS2010-1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1510257253&Signature=k9ajThGExg5Ua7fsxbTfsBOscmQ%3D&response-content-disposition=inline%3B%20filename%3DCPUCIS2010_1.pdf

Deloitte. (2017). *La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información*. Recuperado el 02 de Octubre de 2017, de https://www2.deloitte.com/ec/es/pages/technology-media-and-telecommunications/articles/Cyber-Riesgos-y-Seguirdad-de-la-Informacion.html

El Blog de Javier Megias - Startups, Estrategia y Modelos de Negocio. (11 de Junio de 2013). *Tus peores enemigos: las "best practices" y los estándares | Startups, Estrategia y Modelos de negocio*. Recuperado el 06 de Noviembre de 2017, de https://javiermegias.com/blog/2013/06/tus-peores-enemigos-las-best-practices-y-los-estandares/

Escrivá, G., Gema Romero, S., Rosa María, R., & David, J. (2013). *Seguridad informática.* Madrid, España: Macmillan Iberia, S.A. Recuperado el 24 de Septiembre de 2017, de http://puceftp.puce.edu.ec:2057/lib/pucesp/reader.action?docID=10820963&ppg=217

FayerWayer. (2017). Recuperado el 27 de Octubre de 2017, de https://www.fayerwayer.com/2009/08/hacker-roba-mas-de-130-millones-de-numeros-de-tarjetas-de-credito-y-debito/

FIS. (21 de Mayo de 2017). *Fidelity National Information Services*. Obtenido de https://www.fisglobal.com/

Gestion Calidad. (2017). *Normas y Guías de la Calidad*. Recuperado el 06 de Noviembre de 2017, de http://www.citethisforme.com/es/cite/sources/websiteautociteconfirm

Gómez Vieites, Á. (2014). *Seguridad en equipos informáticos.* Madrid: RA-MA Editorial. Recuperado el 13 de 10 de 2017, de http://puceftp.puce.edu.ec:2057/lib/pucesp/reader.action?docID=11046412&ppg=5

Heyman, S. (29 de 07 de 2015). *Photos, Photos Everywhere*. Recuperado el 13 de 05 de 2017, de The New York Times: https://www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html?_r=0

INCIBE. (13 de Febrero de 2017). *Instituto Nacional de Ciberseguridad*. Recuperado el 24 de Septiembre de 2017, de INCIBE publica el ranking de los 10 principales incidentes de Ciberseguridad a nivel mundial de 2016: https://www.incibe.es/sala-prensa/notas-prensa/incibe-publica-el-ranking-los-10-principales-incidentes-ciberseguridad

ISACA. (2012). *COBIT 5 for Information Security.* Rolling Meadows, Illinois, Estados Unidos: ISACA. Recuperado el 20 de 12 de 2016

ISACA. (2012). *COBIT 5 for Information Security Preview Version.* Recuperado el 05 de Septiembre de 2016, de ISACA: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISACA. (10 de 05 de 2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa.* (M. ISACA, Trad.) Rolling Meadows, IL, Estados Unidos: ISACA. Recuperado el 10 de 05 de 2017

ISACA. (2012). *Cobit 5, Un Marco de Negocio para el Gobierno y Gestion de TI de la empresa.* Estados Unidos. Recuperado el 10 de 05 de 2017

ISO. (2013). *ISO/IEC 27002.* Geneva, Suiza: ISO. Recuperado el 13 de Octubre de 2017

ISO/ IEC 27000. (2016). *Information technology - Segurity techniques - Code of practice for information security controls* (Segunda ed.). Geneva, Suiza: ISO. Recuperado el 18 de Septiembre de 2017

Lapiedra Alcamí, R. D. (2011). *Introducción a la gestión de sistemas de información en la empresa.* Castellón de la Plana: Universitat Jaume I. Servei de Comunicació i Publicacions. Recuperado el 10 de Mayo de 2017

McMillan, R., & Heiser, J. (2017). *Gartner*. Recuperado el 17 de Octubre de 2017, de Five Golden Rules for Creating Effective Security Policy: https://www.gartner.com/doc/2849418?refval=&pcp=mpe#a-115114486

Moore, S. (1 de Octubre de 2015). *Smarter With Gartner*. Recuperado el 26 de 10 de 2017, de https://www.gartner.com/smarterwithgartner/mitigate-risk-with-an-effective-security-policy/

NIST. (2012). *Computer Security Incident Handling Guide.* Gaithersburg: Computer Security Division.

NIST. (2013). *Glossary of Key Information Security Terms.* (R. Kissel, Ed.) Gaithersburg: NIST. Recuperado el 22 de Septiembre de 2017, de http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Osterman Research, Inc. (2016). *Best Practices for Protecting Your Data When Employees Leave Your Company.* Washington. Recuperado el 30 de Octuber de 2017, de http://resources.idgenterprise.com/original/AST-0175464_orwp_0260.pdf

Pearson, S. (2014). *Privacy, Security and Trust.* Bristol: Springer. doi: 10.1007/978-1-4471-4189-1_1

PMI. (2017). *Project Management Institute*. Recuperado el 06 de Noviembre de 2017, de ¿Qué es un estándar?: http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

Pressman, R. S. (2010). *INGENIERÍA DEL SOFTWARE.* México, D. F.: The McGraw-Hill Companies. Recuperado el 20 de Julio de 2017, de http://cotana.informatica.edu.bo/downloads/ld-Ingenieria.de.software.enfoque.practico.7ed.Pressman.PDF

Rouse, M. (2017). *SearchSecurity*. Recuperado el 26 de Octubre de 2017, de http://searchsecurity.techtarget.com/definition/security-policy

Sans. (2017). *SANS - Information Security Resources | Information Security Policy Templates |*. Recuperado el 10 de Octubre de 2017, de https://www.sans.org/security-resources/policies

Soft Warehouse. (30 de Noviembre de 2017). Obtenido de FITBANK: https://fit-bank.com

Tcpsi. (2017). *Gobierno IT - TCP*. Recuperado el 06 de Noviembre de 2017, de http://www.tcpsi.com/servicios/gobierno_ti.htm

Toolkit. (2017). *Módulo 4: Tecnologías de la información*. Recuperado el 08 de Noviembre de 2017, de Estrategias y lineamientos para la seguridad de la información: http://toolkit.cridlac.org/modulo-4-tecnologias-de-la-informacion/unidad-2-funciones-de-gestion-de-las-tecnologias-de-informacion/estrategias-y-lineamientos-para-la-seguridad-de-la-informacion.html

Vieites, Á. G. (2014). *Enciclopedia de la Seguridad Informática.* Madrid: RA-MA, S.A. Editorial y Publicaciones. Recuperado el 11 de Diciembre de 2017, de

https://books.google.com.ec/books?id=Bq8-DwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Wordpress. (23 de Octubre de 2015). *Five Golden Rules for Creating Effective Security Policy*. Recuperado el 31 de Octubre de 2017, de https://shahzadkhurram.wordpress.com/2015/10/23/five-golden-rules-for-creating-effective-security-policy/

Anexos

Introducción

Con el avance tecnológico que se ha venido dando durante los últimos años la seguridad de la información se ha convertido en una de las preocupaciones más críticas en todo tipo de organizaciones.

El presente manual de políticas de seguridad de la información está basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) y en la norma ISO/IEC 27002:2013 para la Gestión de la Seguridad de la Información el cual está conformado por un dominio, un objetivo de control que indica lo que se debe lograr y los distintos controles que se pueden aplicar para alcanzar el objetivo de control.

El manual busca proteger tanto la información como los sistemas de información con adecuados niveles de confidencialidad y protección de la divulgación de información a través de la integridad apropiada en los datos y procesos en sí, de modo que el sistema y los datos estarán a disposición de los usuarios cuando sea necesario. Cabe recalcar que este manual no reemplaza al EGSI ni a la norma ISO/IEC 27002:2013 sino que se han tomado en consideración algunos controles que se consideran prioritarios implementarlos en Soft Warehouse S.A.

Al implementar este manual de políticas incrementará la seguridad de la información en el entorno empresarial de Soft Warehouse S.A.

TABLA DE REFERENCIA

PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - PSI

PSI – D01	POLITICA DE SEGURIDAD
PSI – D02	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
PSI – D03	SEGURIDAD DE LOS RECURSOS HUMANOS
PSI – D04	GESTIÓN DE LOS ACTIVOS
PSI – D05	CONTROL DE ACCESOS
PSI – D06	CRIPTOGRAFÍA
PSI – D07	SEGURIDAD FÍSICA Y AMBIENTAL
PSI – D08	SEGURIDAD DE OPERACIONES
PSI – D09	SEGURIDAD DE LAS COMUNICACIONES
PSI – D10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
PSI – D11	RELACIONES CON PROVEEDORES
PSI – D12	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
PSI – D13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
PSI – D14	CUMPLIMIENTO

Soft Warehouse www.financial-internet-technologies.com	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SOFT WAREHOUSE S.A.**	**PSI-D01**

CAPITULO	**PSI-D01**
DOMINIO	**POLÍTICA DE SEGURIDAD**
OBJETIVO	Proporcionar una directriz que permita solventar los problemas de seguridad de la información en Soft Warehouse S.A. de acuerdo con las leyes y regulaciones vigentes que dispone el estado.

Objetivo de Control: Política de Seguridad de la Información	
Documento de Políticas de Seguridad de la Información	
	a) El Gerente General de Soft Warehouse S.A. dispondrá de este documento de políticas de seguridad de la información que deberá ser aprobado, publicado y comunicado a los empleados y partes externas relacionadas con la compañía.
Revisión de la Política de Seguridad de la Información	
	a) Cada una de las políticas se deberá revisar de forma anual o cuando se realicen cambios significativos en Soft Warehouse S.A. a nivel operativo, tecnológico, económico, entre otros para garantizar la vigencia de la política de seguridad de la información. • Se consideran cambios significativos a la estructura organizacional, innovación en el software, innovación en los procesos, normativa vigente entre otros.

DOMINIO	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
OBJETIVO	Crear una estructura organizativa que dirija la implementación de seguridad de la información dentro del entorno de Soft Warehouse S.A.

Objetivo de Control: Organización Interna	
Compromiso de las autoridades de la compañía con la seguridad de la información	
	a) Efectuar una revisión y control de la puesta en marcha de las normas expuestas en este documento. b) Promover el contenido de este documento mediante el uso de capacitaciones, sensibilización al personal y difusión del mismo. c) Establecer un **Comité de Gestión de la Seguridad de la Información** de la compañía (CSI) y designar a cada uno de los responsables. El comité conformado deberá mantener reuniones de forma periódica o si las circunstancias lo ameritan. Es importante que se lleve un registro de cada una de las reuniones establecidas con su respectiva acta.
Coordinación de la Seguridad de la información	
	La coordinación está a cargo del Comité de Gestión de Seguridad de la Información con las siguientes responsabilidades: a) Mantener la política y normas establecidas por Soft Warehouse S.A. en materia de seguridad de la información. b) Gestionar la aprobación y la puesta en marcha del manual de políticas de seguridad de la información por parte de la Gerencia General de Soft Warehouse S.A. c) Promover la difusión de información en temas de seguridad de la información en la compañía. d) Designar responsables de información en cada área de trabajo que deberá ser formalizado en un documento físico o electrónico. e) Coordinar el proceso de continuidad de los servicios frente a incidentes de seguridad. f) Manejar las iniciativas por parte de los recursos de Soft Warehouse S.A. para incrementar la seguridad de la información. g) Manejar el recurso económico, tecnológico y humano para la gestión de la seguridad de la información. h) Aplicar a medida que sea necesario la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000 en la compañía según la estructura de cada norma. i) Designar formalmente a un responsable como Oficial de Seguridad de la Información quien será el coordinador del CSI. El Oficial de Seguridad de la Información no debe pertenecer al área de Tecnología de la Información

	y será el encargado de reportar a la Gerencia General de Soft Warehouse S.A. j) Designar formalmente al responsable de seguridad del área de Tecnología de la Información en coordinación con el responsable del área de Tecnología de la Información de Soft Warehouse S.A. k) Revisión periódica anual de las políticas respecto a la normativa vigente. l) Aprobar los informes relacionados con temas de seguridad de la información de Soft Warehouse S.A.
Asignación de responsabilidades para la seguridad de la información	
	El **Oficial de Seguridad de la Información** tendrá las siguientes responsabilidades: a) Desarrollar procedimientos para poder gestionar los incidentes de seguridad y mantener a Soft Warehouse S.A. a salvo de amenazas internas como externas. b) Identificar las herramientas y servicios adecuados a ser implementados en Soft Warehouse S.A. para la detección de amenazas. c) Desarrollar un plan de capacitaciones para concientizar a cada uno de los empleados en materia de seguridad, accesos a la información, medios de almacenamiento y formar una cultura de seguridad. d) Monitorear las amenazas para la toma de decisiones preventivas. e) Supervisar la difusión y distribución de la información dentro de la compañía y fuera de la compañía. f) Comunicarse con todo el personal sobre los métodos o procedimientos que usan los cibercriminales para obtener información de manera ilícita y como sus acciones pueden conducir a la violación de datos. g) Definir y realizar la documentación adecuada donde se establezcan métodos de prevención frente al acceso no autorizado a los activos, sistemas de información y zonas de trabajo. h) Realizar un seguimiento de las normas, procedimientos y controles de seguridad establecidos en Soft Warehouse S.A. i) Mantener reuniones periódicas con el Comité de Seguridad de la Información o cuando la situación lo amerite, además se debe llevar un registro de las reuniones. j) Definir la clasificación de la información. El **Responsable de Seguridad del Área de Tecnología de la Información** tendrá las siguientes responsabilidades: a) Verificar que toda la documentación (procedimientos, diagramas, procesos, operaciones entre otros) física como de forma digital se encuentre actualizada. b) Respetar los procedimientos establecidos para tratar los incidentes de seguridad. c) Monitorear la capacidad de los sistemas de operación para combatir amenazas futuras. d) Monitorear la adquisición de respaldos de la información. e) Desarrollar procedimientos para la comunicación de fallas en el procesamiento de la información o sistemas de comunicaciones. f) Implementar controles de seguridad basados en buenas prácticas, estándares y normas internacionales.

	g) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento como por ejemplo (disco duros, flash memory) y documentación impresa. Además se debe verificar la eliminación de la misma cuando haya acabado su tiempo de vida útil. h) Manejar los incidentes de seguridad informática de acuerdo a los procedimientos establecidos.
Proceso de autorización para nuevos servicios de procesamiento de la información.	
	a) Definir un responsable a cargo de los nuevos servicios a implementar que se encargará de mantener un control de accesos de los usuarios según sea su propósito dentro del sistema. b) La autorización se solicitará al Oficial de seguridad de la información para mantener el cumplimento de las políticas expuestas en este documento. c) Verificar el hardware y software de la compañía para asegurar que son compatibles y cumplen con los requisitos necesarios para operar con los componentes del sistema. d) Identificar e implementar controles necesarios cuando se manejan servicios de procesamiento de información personales, privados, o de terceros para evitar un nuevo ingreso de vulnerabilidades en Soft Warehouse S.A.
Contacto con grupos de intereses especiales	
	a) Obtener conocimiento sobre las mejores prácticas y mantenerse al día con información relevante. b) Garantizar la compresión sobre seguridad de la información sea completa y con información actual. c) Recibir información actual de los ataques y vulnerabilidades más frecuentes en las empresas de país y del mundo. d) Buscar asesoramiento especializado a profesionales en temas de seguridad de la información. e) Compartir e intercambiar información entre los recursos de Soft Warehouse S.A. sobre nuevas tecnologías, productos, amenazas o vulnerabilidades. f) Proporcionar puntos de enlace adecuados cuando se trata de incidentes de seguridad de la información.
Seguridad de la información en la gestión de proyectos	
	a) Los objetivos de seguridad de la información se deben incluir en los objetivos del proyecto. b) Realizar una evaluación de riesgos de seguridad de la información en una etapa temprana del proyecto para poder identificar los controles necesarios. c) Identificar riesgos de la seguridad de la información en cada una de las fases de la metodología de la gestión de proyectos.
Objetivo de control: Dispositivos móviles y trabajo remoto	
Política de dispositivo móvil	
	a) No usar dispositivos móviles en lugares públicos, sala de reuniones y otros lugares sin protección, con el fin de evitar el acceso no autorizado o divulgación de la información.

	b) Los dispositivos móviles deben estar físicamente protegidos contra el robo permitiendo el borrado total del dispositivo. c) Los dispositivos móviles que suministra Soft Warehouse S.A. deben bloquearse físicamente para resguardar la información por medio de un código o un patrón de ingreso. Cuando se manejan dispositivos móviles como activo de Soft Warehouse S.A. se debe considerar: a) La separación del uso privado y del negocio en el dispositivo, incluido el software para respaldar tal separación y protección de los datos. b) Proporcionar acceso a la información del negocio solo después de que el usuario haya firmado un acuerdo de usuario final reconociendo sus deberes. c) Eliminación del dispositivo por parte de la compañía en caso de robo, pérdida o cuando ya no está autorizado para su uso.
Trabajo remoto	
	a) Solo el Gerente General de Soft Warehouse S.A. podrá autorizar la modalidad de trabajo remoto. Cuando se realice la modalidad de trabajo remoto se debe: • Tener en cuenta la seguridad física del entorno donde se ejecutará el trabajo. • Mantener requisitos de seguridad de las comunicaciones cuando se realice el acceso remoto a los sistemas internos de Soft Warehouse S.A. • Evitar la conexión a redes inalámbricas que no presten seguridad de acceso. • Configurar los requisitos de firewall y protección contra malware. • Tomar en consideración la privacidad del espacio y la no divulgación de información confidencial con relación a terceras personas presentes en el lugar. b) Permitir al personal realizar trabajo remoto en casos que se deba brindar servicios de implantación o soporte a clientes, debe existir una petición de cliente y autorización previa del líder del proyecto adicional a la del Gerente General de Soft Warehouse S.A.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**SEGURIDAD DE LOS RECURSOS HUMANOS**
OBJETIVO	Asegurar que el personal de Soft Warehouse S.A. conozca sus responsabilidades y sean capaces de desenvolverse en las actividades para las que son designadas.

Objetivo de Control: Antes de la contratación	
Investigación de antecedentes	
	a) Verificar el curriculum vitae del postulante lo que incluye la verificación de la identificación (cédula o pasaporte) comprobación de los títulos académicos y profesionales, revisión de antecedentes penales, y recomendaciones laborales. b) Cuando un recurso es contratado para desempeñar el papel de seguridad de la información específica, Soft Warehouse S.A. debe asegurarse que: • El recurso tiene los conocimientos necesarios para llevar a cabo la función de seguridad. c) Se debe informar al personal acerca del procedimiento de selección del nuevo recurso con anterioridad.
Términos y condiciones de contratación	
	a) Antes de brindar acceso a la información confidencial de Soft Warehouse S.A. se deben firmar acuerdos de confidencialidad o acuerdos de no-divulgación al recurso. b) Soft Warehouse S.A. debe asegurarse que el recurso está de acuerdo con los términos y condiciones que establece la compañía para el cumplimiento de las normas de seguridad de la información. c) Informar sobre los derechos y responsabilidades legales que posee el empleado o contratista sobre la protección de datos, el uso adecuado de los equipos de Soft Warehouse S.A., instalaciones; evidenciando lo actuado a través de registros, informes o actas. d) Realizar acuerdos de confidencialidad con los proveedores.
Objetivo de control: Durante la contratación	
Responsabilidades de gestión	
	a) Estar de acuerdo con sus roles y responsabilidades de seguridad de la información antes de ser concedido el acceso a los sistemas de información o de información confidencial de Soft Warehouse S.A. b) Lograr un nivel de conciencia orientado a la seguridad de la información para poder cumplir sus funciones y responsabilidades con éxito en Soft Warehouse S.A. c) Cumplir con las políticas de seguridad de la información que dispone Soft Warehouse S.A. y con los métodos de trabajo.
Concienciación, formación y capacitación en seguridad de la información	

	a) Todo el personal Soft Warehouse S.A. debe recibir capacitaciones enfocadas a la seguridad de la información con el objetivo de dar a conocer sus responsabilidades en materia de seguridad de la información. b) Realizar programas de sensibilización los cuales deben incluir actividades que permita al personal de Soft Warehouse S.A. conocer más acerca de la seguridad de la información por medio de afiches, boletines, entre otros. • Los programas de sensibilización deben ser programados de manera permanente ya que Soft Warehouse S.A. constantemente está enrolando a nuevo personal. • Los programas de sensibilización deben planificarse teniendo en cuenta cada una de las funciones de los empleados de Soft Warehouse S.A. • Los programas de sensibilización deben ser actualizados regularmente para mantener concordancia con las políticas y procedimientos de Soft Warehouse S.A. • Los programas de sensibilización deben asegurar que los participantes entiendan los temas tratados. c) La sensibilización al personal sobre una cultura de seguridad se puede realizar mediante charlas, aprendizaje a distancia, mediante la web para respetar el ritmo de trabajo del personal. La educación y formación de seguridad también debe cubrir los siguientes aspectos como: a) Indicar el compromiso con la seguridad de la información en Soft Warehouse S.A. b) La responsabilidad de conocer y cumplir con las directrices de seguridad tal como se definen en las políticas, leyes, reglamentos contratos y acuerdos. c) La responsabilidad personal por las acciones de uno mismo para asegurar y proteger la información confidencial de Soft Warehouse S.A. y las partes externas con las que se trabaja. d) Tener puntos de contacto dentro de Soft Warehouse S.A. para obtener información adicional y asesoramiento en materia de seguridad de la información lo que incluye material educativo.
Proceso disciplinario	
	a) El proceso disciplinario debe asegurar un tratamiento correcto y justo para el empleado que ha cometido infracciones en materia de seguridad de la información. Se debe iniciar una comprobación previa de que se ha producido una violación de la seguridad en Soft Warehouse S.A. b) El proceso disciplinario debe considerar factores tales como la naturaleza y gravedad de la infracción y su impacto en Soft Warehouse S.A., si es la primera ocasión o es reincidencia del empleado, si fue debidamente capacitado con anterioridad o no. c) El proceso disciplinario debe ser utilizado como un método de disuasión frente al personal con el objetivo de que no violen las políticas y procedimientos de seguridad de la información de Soft Warehouse S.A.

	y cualquier otra infracción o violación que pueda requerir acciones inmediatas.
Objetivo de Control: Cierre o cambio de puesto de trabajo	
Cese o cambio de puesto de trabajo	
	a) Los cambios de responsabilidad o puesto deben gestionarse como la terminación de la actual responsabilidad o puesto combinado con el inicio de la nueva responsabilidad o puesto. b) En la fase de terminación del contrato laboral o cambio de puesto se debe realizar la transferencia de documentación e información de la que fue responsable en el lapso de tiempo de trabajo al nuevo recurso, en el caso de que no se haya designado un nuevo recurso se deberá entregar al Oficial de Seguridad de la Información.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**GESTIÓN DE LOS ACTIVOS**
OBJETIVO	Identificar los activos que posee Soft Warehouse S.A. y definir a los responsables que se encarguen de la protección apropiada.

Objetivo de Control: Responsabilidad sobre los activos	
Inventario de Activos	
	a) Soft Warehouse S.A. debe identificar los activos relevantes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida debe incluir creación, procesamiento, almacenamiento, trasmisión, eliminación, y destrucción. b) El inventario de activos debe ser preciso, actualizado, consistente y alineado con otros inventarios. Se deben inventariar los siguientes activos: • Inventario de activos primarios en formatos físicos y/o electrónicos. • Inventario de activos de soporte de Hardware. • Inventario de activos de soporte de Software. • Inventario de activos de soporte de redes. • Inventariar los activos referentes a la estructura organizacional. c) Considerar la ISO/IEC 27005 proporciona una clasificación de activos que pueden ser consideraros para el inventario de la compañía. d) Se debe actualizar la información del inventario no mayor a seis meses.
Propiedad de los Activos	
	a) Asignar un responsable a los activos o grupos de activos, esto no implica que el responsable tenga derecho de propiedad de los activos como por ejemplo (discos duros, servidores, monitores, routers) El responsable del activo tendrá las siguientes funciones: • Realizar un inventario de los activos designados y actualizarlo a medida que sea necesario. • Elaborar reglas de uso aceptable del mismo e implementarlas previa la autorización de la autoridad correspondiente. • Seleccionar, documentar y mantener actualizada la información y definir los permisos de acceso a la misma. b) Asegurar que los activos estén inventariados. c) Asegurar que los activos estén debidamente clasificados y protegidos. d) Revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, tomando en cuenta las políticas de control de acceso aplicables. e) Garantizar un manejo adecuado cuando el activo es eliminado o destruido.

Uso aceptable de los activos	
	a) El personal y usuarios externos que usan o tienen acceso a los activos de Soft Warehouse S.A. deben tener en cuenta los requisitos de seguridad de la información. b) El personal y usuarios externos deben ser responsables del uso de cualquier recurso de procesamiento de información. c) La información y documentos realizados, enviados desde Soft Warehouse S.A. por cualquier medio o herramienta electrónica se considera propiedad de la compañía.
Devolución de los activos	
	a) Todos los empleados y usuarios externos de Soft Warehouse S.A. están obligados a pasar por un proceso de devolución de activos como parte de su terminación de relación laboral. b) En los casos en que un empleado o un usuario externo es importante para las operaciones en curso, esa información debe documentarse y transferirse a Soft Warehouse S.A. c) Durante el período de aviso de terminación, la compañía debe controlar la copia no autorizada de información relevante (por ejemplo, propiedad intelectual) por parte de empleados y contratistas que terminaron su relación de dependencia con Soft Warehouse S.A.
Objetivo de Control: Clasificación de la información	
Directrices de clasificación	
	a) La información debe ser clasificada en pública y confidencial. b) Tomar en cuenta la relevancia jurídica, el nivel de confidencialidad y el valor de la información para Soft Warehouse S.A. a. Evaluar la protección de la información por medio de la confidencialidad, integridad y disponibilidad. c) La clasificación de la información se revisará anualmente o cada 3 años.
Etiquetado y manipulación de la información	
	a) Los procedimientos para el etiquetado de la información deben cubrir la información y sus activos relacionados en forma física y formatos electrónicos. b) Las etiquetas deben ser fácilmente reconocibles. c) El personal debe estar al tanto de los procedimientos de etiquetado. d) La producción de los sistemas que contienen información clasificada como sensible o crítica debe llevar una etiqueta de clasificación apropiada. e) Los responsables de los activos supervisarán el etiquetado de los activos. f) En el caso de etiquetas físicas los responsables de los activos deberán verificar que las etiquetas estén rotulados y legibles. g) Cuando se destruye un activo se debe mantener en el inventario respectivo y se debe indicar el estatus en el que se encuentra. h) El almacenamiento de los activos de TI se deben hacer de acuerdo a las especificaciones del fabricante. i) Protección de los respaldos temporales o permanentes en otro sitio.

Objetivo de Control: Manejo de los soportes de almacenamiento	
Gestión de activos extraíbles	
	a) Todos los activos deben almacenarse en un entorno seguro y protegido, de acuerdo con los fabricantes. b) Si la confidencialidad o la integridad de los datos son consideraciones importantes, las técnicas criptográficas deberían ser utilizado para proteger datos en medios extraíbles. c) Almacenar copias múltiples de datos valiosos en medios separados para reducir aún más el riesgo de pérdida o daño de datos fortuitos. d) El registro de medios extraíbles limita la pérdida de datos. e) Las unidades de medios extraíbles solo deben habilitarse si existe una razón para hacerlo. f) Cuando sea necesario utilizar medios extraíbles, la transferencia de información a dichos medios debería ser monitoreado.
Eliminación de activos	
	a) Los activos que contienen información confidencial de Soft Warehouse S.A deben desecharse de forma segura por ejemplo (incineración o trituración, o borrado de datos). b) Definir procedimientos para identificar los artículos que podrían requerir una eliminación segura. • Recolectar todos los artículos y eliminarlos de manera segura, en lugar de hacerlo por separado. c) Si se dispone de servicios de recolección, tener cuidado en seleccionar una parte externa adecuada para la eliminación de los artículos. d) Para el caso de la eliminación de elementos sensibles se debe registrar para mantener un control.
Soportes físicos en tránsito	
	a) Se debe utilizar transporte seguro o mensajeros confiables. b) Acordar una lista de correos autorizados con la administración. c) Desarrollar procedimientos para verificar la identificaron de los correos. d) El embalaje debe ser suficiente seguro para proteger el contenido de cualquier daño físico que pueda surgir durante el tránsito por ejemplo (proteger contra cualquier factor ambiental, exposición al sol, humedad, campos electromagnéticos).

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**CONTROL DE ACCESOS**
OBJETIVO	Controlar el acceso autorizado y no autorizado a los sistemas de información de Soft Warehouse S.A.

Objetivo de Control: Requisitos de negocio para el control de accesos.	
Política de control de accesos	
	a) Gestionar el acceso de los usuarios teniendo en cuenta el rol, actividades, tareas y responsabilidades; factores en base a los que se definirán los derechos de acceso a información que le pertenecen al usuario. b) Los derechos de acceso a la información serán otorgados en base a un modelo de conocimiento de información mínimo, es decir, dar acceso a la información lo mínimo necesario para poder cumplir con sus responsabilidades. Necesidad de tener y necesidad de saber. c) Los accesos de información deben ser coordinados y aprobados dentro de cada función de Soft Warehouse S.A., esta tarea recae en los líderes o jefes de cada función y los dueños de activos. d) Los derechos de acceso a la información deberán respetar las normas de protección de información crítica con el fin de resguardar la integridad y confidencialidad de la misma. e) Con el fin de mantener la continuidad aceptable, toda función que se relaciona con la gestión de información crítica debe contar con un encargado principal y un alterno. f) Todo acceso a la información debe estar evidenciado en un registro que permita identificar el usuario y la razón de uso de la cierta información. g) Manejar un proceso que registre los cambios de privilegios de acceso a información y registre cuando se debe ejecutar dicho cambio.
Control de acceso a las redes y servicios asociados	
	a) Definir procedimientos de autorización para definir quién puede acceder a que redes y servicios asociados. b) El personal solo debe tener acceso a la red y a los servicios que han sido autorizados para su uso. c) Contar con una red para invitados. • Asegurar que todo invitado únicamente acceda a esta red. • Mantener la red de invitados independiente del resto de redes locales. • La contraseña de acceso a esta red deberá cambiarse en intervalos de dos meses. d) Soft Warehouse S.A. debe contar con controles en servicios y redes para resguardar los accesos a las mismas. e) Se debe contar con un Log de todo intento de acceso a los servicios y redes de Soft Warehouse S.A.

	f) Solicitar requisitos de autentificación de usuario para acceder a los diversos servicios de red. g) Realizar un monitoreo del uso de los servicios de red.
Objetivo de Control: Gestión de acceso de usuario	
Registro de usuario y cancelación de registro	
	a) Implementar un proceso formal de registro y eliminación de usuarios, el cual debe ser documentado y difundido, en el cual se refleje los pasos y responsables para: • Definir un administrador de accesos que se encargue de controlar los perfiles y roles de usuario. • Realizar un documento donde se registre el acceso de usuarios internos y externos que contenga: Nombre de la persona que solicita el acceso, ambiente al que desea ingresar, base de datos a utilizar, fecha de expiración, tiempo estimado de utilización y motivo estimado. • Asignar y habilitar el acceso de usuarios. • Modificar accesos de usuarios. • Deshabilitar o eliminar el acceso a los usuarios que abandonan la compañía. • Identificar y eliminar periódicamente el acceso de usuarios redundantes. • Garantizar que los usuarios redundantes no se envíen a otros usuarios. • Suspender el acceso al personal que solicita vacaciones o permiso temporal. • Asignar accesos temporales a terceras partes de acuerdo a su tiempo de permanencia en Soft Warehouse S.A.
Gestión de derechos de acceso privilegiado	
	a) La asignación de derechos de acceso privilegiado debe controlarse a través de un proceso de autorización formal. b) Los derechos de acceso privilegiado deben asignarse a los usuarios dependiendo del motivo y la necesidad de uso. c) Mantener un registro de los responsables de activos críticos y accesos a la información de los mismos. d) Designar un responsable alterno para la gestión de los activos críticos, con el fin de mantener un nivel aceptable de la continuidad de Soft Warehouse S.A. e) Se deberá hacer una petición formal en casos que personal que no sea responsable del activo desee acceder a dicha información para realizar funciones que modifiquen dicha información. f) La petición de acceso debe entregarse al responsable del activo crítico y a un resguardo de información, con fin de mantener un registro de toda petición. g) La petición únicamente podrá ser aprobada o rechazada por el responsable del activo crítico. h) Debe mantenerse un registro de peticiones de acceso a sistemas, bases de datos y aplicaciones donde se encuentre información crítica y/o confidencial.

	i) En caso de ser una emergencia o situación extraordinaria la Gerencia puede solicitar de forma escrita que se autorice a un recurso el acceso a activos críticos o información confidencial. j) Todo acceso otorgado, mediante petición formal, deberá ser supervisado por el responsable del activo crítico con la finalidad de supervisar las actividades realizadas con el mismo y asegurar la información del mismo. k) Mantener un documento actualizado del proceso de autorización de acceso y un registro de todos los privilegios que son asignados a los recursos de Soft Warehouse S.A. l) Definir los requisitos para la expiración de los derechos de acceso privilegiado. m) Revisar regularmente los accesos privilegiados a los usuarios para verificar si están de acuerdo con sus deberes dentro de Soft Warehouse S.A. n) Definir procedimientos para evitar el uso no autorizado de accesos privilegiados.
Revisión de los derechos de acceso de los usuarios	
	a) La persona responsable de los activos debe realizar una revisión de los derechos de acceso de los usuarios regularmente, máximo en 30 días. b) Los derechos de acceso de los usuarios deberán revisarse y reasignarse al pasar de un rol a otro dentro de la misma compañía. c) Las autorizaciones para derechos de acceso privilegiado deben revisarse frecuentemente. d) La asignación de privilegios deben verificarse regularmente para garantizar que los privilegios no autorizados no han sido divulgados. e) Los cambios que ser realicen en las cuentas con privilegios deben registrarse con fecha y motivo para su revisión periódica
Eliminación o ajuste de los derechos de acceso	
	a) Durante el periodo de finalización de relaciones laborales de empleados, proveedores y terceros con Soft Warehouse S.A. se debe tomar en cuenta la eliminación de los derechos de acceso de los mismos.
Objetivo de Control: Responsabilidades del usuario	
Uso de información confidencial para la autenticación	
	a) El personal debe estar obligado a seguir las prácticas de Soft Warehouse S.A. en el uso de la información de autenticación secreta. b) Mantener la confidencialidad de la información secreta de autenticación, asegurando que no se divulgue a las distintas áreas de trabajo incluyendo personas de autoridad. c) Evitar mantener un registro (por ejemplo, en papel, archivo de software o dispositivo de mano) de autenticación secreta, a menos que se pueda almacenar de forma segura y se haya aprobado el método de almacenamiento (por ejemplo, bóveda de contraseña). d) Cuando las contraseñas se usan como información de autenticación secreta, se debe establecer una contraseña: • Con una longitud mínima de caracteres. • Usar caracteres especiales. • No se deben incluir nombres, números de teléfono, fechas de nacimiento.

	• No debe contener palabras incluidas en el diccionario. • Debe ser libre de caracteres consecutivos idénticos, totalmente numéricos o complete alfabéticos. • Si la contraseña es temporal, debe pedir el cambio en el primer inicio de sesión. e) No se debe compartir la información de autenticación secreta personal a otros usuarios. f) Garantizar la protección adecuada de las contraseñas cuando se usan contraseñas como autenticación secreta información en el caso de procedimientos automatizados en el caso de inicio de sesión y el almacenamiento automático. g) No usar la información de autenticación para fines comerciales o no comerciales.
Objetivo de Control: Control de acceso a sistemas y aplicaciones	
Restricción del acceso a la información	
	a) Se debe proporcionar menús para controlar el acceso a las funciones de las aplicaciones o ambientes. b) Controlar a qué datos puede acceder un usuario particular. c) Controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, eliminar y ejecutar d) Controlar los derechos de acceso de otras aplicaciones. e) Limitar la información contenida de los ambientes o aplicaciones.
Procedimientos de inicio de sesión seguros	
	a) El procedimiento para el inicio de sesión no debe mostrar información sobre el sistema o aplicación, para evitar mostrar al usuario no autorizado cualquier información que pueda atentar contra la integridad de Soft Warehouse S.A. b) El procedimiento de inicio de sesión debe desplegar un mensaje de alerta advirtiendo que solo los usuarios autorizados pueden acceder al ambiente o sistema. c) Durante el procedimiento de inicio de sesión no se deben proporcionar mensajes de ayuda a un usuario no autorizado. d) Corroborar la información de inicio de sesión cuando el usuario haya completado todos los datos de entrada sugeridos, si ocurre un error en el ingreso, el sistema no debe indicar que datos son correctos o incorrectos. e) Mantener un registro de los intentos de inicios de sesión fallidos y exitosos. • Registrar la fecha y hora de inicio de sesión exitoso. • Registrar el detalle del intento fallido de inicio de sesión desde el último inicio de sesión exitoso. f) Durante el procedimiento de inicio de sesión no debe mostrar la contraseña ingresada. g) Finalizar sesiones inactivas después de un periodo de inactividad definido, especialmente en lugares de alto riesgo como áreas públicas o externas fuera de la seguridad de Soft Warehouse S.A. o en dispositivos móviles. h) Establecer un tiempo determinado de conexión para garantizar mayor seguridad en las aplicaciones o ambientes de alto riesgo y reducir la oportunidad de acceso no autorizado.

Sistema de gestión de contraseñas	
	a) El sistema de gestión de contraseñas debe ser interactivo, simple y debe garantizar calidad en las contraseñas. b) El sistema de gestión de contraseñas debe ser controlado por un administrador y dos personas alternas. • El administrador debe realizar un respaldo diario de la información almacenada en el sistema, principalmente de las cuentas. c) El sistema de gestión de contraseñas que se utilice debe ser multiusuario con gestión de usuarios, grupos y perfiles. d) El sistema de gestión de contraseñas debe: • Obligar a los usuarios a cambiar su contraseña en el primer inicio de sesión. • Mantener un registro de las contraseñas usadas anteriormente y evitar la reutilización de las mismas. • No debe mostrar contraseñas en la pantalla cuando se realiza el ingreso. • Almacenar las contraseñas de forma protegida, almacenamiento cifrado. • El protocolo web de comunicación debe ser seguro, es decir (https). • Debe permitir la compartición segura de contraseñas. • Debe permitir para casos de emergencia que el administrador otorgue permisos extraordinarios a contraseñas previamente almacenadas en el sistema a otros usuarios con fin de mantener un alto nivel de continuidad de negocio. Todo esto bajo autorización de la gerencia. • Debe permitir realizar copias de seguridad de las cuentas almacenadas.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**CRIPTOGRAFÍA**
OBJETIVO	Incorporar el uso de la criptografía para proteger la disponibilidad, confiabilidad, e integridad de la información de Soft Warehouse S.A.

Objetivo de Control: Controles Criptográficos	
Política sobre el uso de controles criptográficos	
	a) Definir el nivel de protección que se requiere en los datos que se van a almacenar en el sistema, teniendo en cuenta: el tipo, fortaleza y la calidad del algoritmo de encriptación. b) Utilizar controles criptográficos para la protección de claves de acceso a los ambientes, servidores, datos, servicios. • Las claves deben ser almacenadas de manera cifrada en la base de datos. c) Definir procedimientos de administración de claves en caso de pérdida, reemplazo o daño de clave. d) Definir los algoritmos de cifrado que se van a utilizar en la Soft Warehouse S.A. dependiendo de los controles que se desean aplicar. e) Utilizar controles criptográficos cuando se desea transmitir información confidencial fuera de Soft Warehouse S.A. f) Utilizar certificados electrónicos reconocidos por el Estado para la firma de cualquier documento, transacción que interactúan con el sistema, aplicaciones entre otros. • Los certificados deben ser emitidos bajo estándares y deben ser organizaciones reconocidas con controles y procedimientos idóneos.
Gestión de claves	
	a) Proteger todas las claves sin excepciones contra modificación destrucción, copia o divulgación no autorizada. b) Protección adecuada de claves por medio de aplicaciones que generar, almacenan y archivan claves. c) Cambiar o actualizar las claves de manera periódica. d) Emitir y obtener certificados de clave pública. e) Proporcionar la clave a los usuarios y la forma de activar y confirmar la recepción de la clave, por medio del correo electrónico se validará la entrega de la clave. Es obligatorio que se cambie la clave predeterminada. f) Definir los procedimientos para cambiar o actualizar las claves y las reglas sobre cuando cambiarles y cómo hacerlo. g) Mantener un registro actualizado para la gestión de claves.

	h) Destrucción de claves cuando se dejen de utilizar. i) Recuperar claves pérdidas o corruptas.

Soft Warehouse www.financial-internet-technologies.com	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SOFT WAREHOUSE S.A.**	**PSI-D07**

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**SEGURIDAD FÍSICA Y AMBIENTAL**
OBJETIVO	Evitar el acceso físico no autorizado, daños a las instalaciones de procesamiento de información de Soft Warehouse S.A.

Objetivo de Control: Áreas Seguras	
Perímetro de seguridad física	
	Las siguientes pautas se deben considerar en los perímetros de seguridad: a) Se deben definir perímetros de seguridad en Soft Warehouse S.A. dependiendo de los requisitos de seguridad de los activos. b) Las instalaciones deben estar físicamente estables, no deben existir huecos o fisuras, deben estar físicamente protegidas contra el acceso no autorizado con mecanismos de control. • Los mecanismos de control son barreras, alarmas, cerraduras. c) Se debe disponer de un área de recepción para controlar el acceso físico al edificio, cabe recalcar que el acceso debe ser restringido al personal no autorizado. d) Disponer de alarmas contra incendios y puertas de evacuación empleando la debida señalización basada en estándares nacionales e internacionales. e) Se debe instalar un sistema de vigilancia para cubrir las puertas externas y ventanas accesibles, la cobertura se debe extender a la sala de reuniones y el pasillo. f) Las instalaciones de procesamiento de información que están administradas por Soft Warehouse S.A. deben estar físicamente separadas de las instalaciones administradas por terceros externos.
Controles físicos de entrada	
	a) Mantener un registro que contenga la fecha de entrada, hora de entrada y hora de salida de las personas externas a la compañía, visitantes o clientes. • Se puede utilizar un libro de registro físico o una plantilla electrónica. Todos los accesos deben monitorearse de manera segura. b) La identidad de los visitantes o clientes debe ser autenticada por medio de la cédula de identidad.

	c) Se debe supervisar la entrada de visitantes o clientes a menos que su acceso haya sido aproado con anterioridad. d) Se debe controlar que todos los empleados, visitantes, clientes y partes externas deban llevar un tipo de identificación o gafete de identificación visible. e) Los derechos de acceso a áreas seguras deben actualizarse periódicamente, mismos que serán documentados y firmados por el responsable.
Asegurar oficinas, habitaciones e instalaciones	
	a) Mantener las puertas y ventanas cerradas cuando no haya personal dentro de la oficina o vigilancia. b) Posicionar las impresoras, copiadoras, scanner en un área protegida. c) Controlar las instalaciones claves con el fin de evitar el acceso a público no autorizado. d) Utilizar cerraduras reforzadas en las puertas de la oficina.
Protección contra amenazas externas y ambientales	
	a) Se debe obtener asesoramiento especializado al personal de emergencia (bomberos, policías, militares) de que procedimientos seguir en caso de terremotos, inundaciones, incendios, temblores o desastres provocados por el hombre. b) Realizar una inspección de las instalaciones eléctricas y brindar el mantenimiento necesario si corresponde. c) Realizar una inspección de los ductos de ventilación dentro de cada oficina y brindar el mantenimiento necesario si corresponde. d) Realizar mantenimiento de los calefactores eléctricos situados dentro de las oficinas.
El trabajo en áreas seguras	
	a) El personal debe conocer la existencia de áreas seguras. b) Se debe controlar el trabajo no supervisado en áreas seguras, tanto por razones de seguridad como para evitar actividades maliciosas que atenten contra la integridad de Soft Warehouse S.A. c) Las áreas seguras desocupadas deben estar cerradas y deben ser revisadas periódicamente. d) Los equipos como cámaras de video, micrófonos, equipos de grabación, cámaras en dispositivos móviles no son permitidos a menos que estén autorizados.
Objetivo de Control: Seguridad de los equipos	
Ubicación y protección de equipos	
	a) Ubicar los equipos como (servidores) en un área restringida para minimizar el acceso innecesario. b) Las instalaciones donde se manejen datos confidenciales deben colocarse fuera del alcance de personas no autorizadas para evitar que vean información durante su uso. c) Salvaguardar los artículos que requieren protección especial. d) Las instalaciones de almacenamiento deben estar aseguradas para evitar el acceso no autorizado.

	e) Adoptar controles para minimizar el riesgo de posibles amenazas físicas o ambientales como: explosivos, fuego, humo, polvo, interferencia de comunicaciones, radiación. f) Establecer reglas para no comer, beber, fumar, en áreas de procesamiento de información. g) Detectar condiciones que podrían afectar el funcionamiento de las instalaciones de procesamiento de información por caso de humedad y temperatura.
Servicios de suministro	
	a) Documentar los suministros de la compañía como (agua, calefacción, aire acondicionado, ventilación, servicios de electricidad) b) Poseer suministros de energía sin interrupción (UPS). c) Monitorizar los sistemas de suministro de energía.
Seguridad del cableado	
	a) Proteger el cableado por medio de un riel para cables o cualquier otro mecanismo que evite el daño y desgaste del mismo. b) Se recomienda la utilización de líneas de energía y telecomunicaciones subterráneas. c) Rotular el cableado bajo normas nacionales e internacionales para disminuir los errores de manipulación. d) Los cables de energía y los cables de comunicaciones deben estar separados de modo que se pueda evitar la interferencia. e) Documentar la distribución del cableado y conexiones alámbricas e inalámbricas de Soft Warehouse S.A.
Mantenimiento de los equipos	
	a) Solo el personal de mantenimiento puede llevar a cabo la reparación de los equipos en mal estado. b) Se debe mantener un registro de las fallas y de todo el mantenimiento preventivo y correctivo. c) Antes de poner el equipo en ejecución, garantizar que no ha sido manipulado, alterado o que funciona incorrectamente. d) Cumplir con los requisitos de mantenimiento que sugiere el fabricante del equipo. e) Cuando sea necesario la información debe eliminarse del equipo, generando un respaldo del mismo.
Eliminación de activos	
	a) Se debe establecer un límite de tiempo para la eliminación de activos. b) Los activos deben registrarse como retirados de Soft Warehouse S.A. cuando sea necesario y apropiado. c) Se deben documentar la identidad, función, y afiliación de la persona que maneja o usa los activos por eliminar.
Seguridad de los equipos y activos fuera de las instalaciones	
	a) Supervisar los equipos y medios que se saquen de Soft Warehouse S.A. en ambientes públicos. b) Revisar las instrucciones de los fabricantes para proteger el equipo en cualquier ambiente.

	c) Supervisar el trabajo que se realiza en equipos o medios fuera de Soft Warehouse S.A. mediante una evaluación de riesgos. Se aplicarán los controles adecuados según correspondan. d) Se debe mantener un registro de cadena de custodia del equipo si se transfiere entre diferentes personas o partes externas. • El registro debe incluir los nombres personales y el de la organización a la que pertenecen los responsables del equipo.
Eliminación segura o reutilización de equipo	
	a) Los equipos dañados dentro de Soft Warehouse S.A. se deben evaluar para determinar si deben destruirse físicamente en lugar de repararlos o desecharlos. • La información se puede comprometer a través de la eliminación descuidada. b) Se debe realizar un cifrado del disco ya que reduce la divulgación de información confidencial. c) Solamente se puede desechar un equipo cuando: • El proceso de encriptación es suficientemente fuerte y cubre todo el disco (incluido el espacio libre). • Las claves de cifrado son extensas. • Las claves de cifrado se mantienen confidenciales.
Equipo informático de usuario desatendido	
	a) El equipo desatendido debe desconectarse de las aplicaciones, ambientes o servicios de red cuando ya no sean necesarios. b) Se debe finalizar sesiones activas dentro del equipo desatendido con un mecanismo de bloqueo por ejemplo con un protector de pantalla protegido por contraseña. c) Proteger las computadoras o dispositivos móviles del uso no autorizado mediante un control por medio de contraseñas o tokens.
Política de escritorio y pantalla clara	
	a) La información comercial sensible o crítica de Soft Warehouse S.A. en papel o en medios de almacenamiento electrónico debe ser resguardada con las medidas de seguridad pertinentes en un lugar como una caja fuerte o armario y tomarlo cuando se requiera. b) Cuando el ordenador no esté en uso se debe dejar desconectado o protegidos con la pantalla y teclado bloqueados mediante una contraseña o mecanismo de autentificación. c) Mantener la pantalla del escritorio clara para reducir los riesgos de acceso no autorizado y daño de la información durante y fuera de las horas normales de trabajo en Soft Warehouse S.A.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**SEGURIDAD DE OPERACIONES**
OBJETIVO	Asegurar que se manejen las operaciones correctas y seguras en el ambiente de Soft Warehouse S.A.

Objetivo de control: Responsabilidades y procedimientos de operación	
Documentación de procedimientos de operación	
	a) Documentar el procesamiento y manejo de información tanto automatizada como manual. b) Documentar la configuración de los sistemas. c) Documentar los requisitos de programación, incluyendo las dependencias con otros sistemas. d) Documentar el procedimiento para manejar errores, restricciones y excepciones que pueden ocurrir durante la ejecución. e) Documentar el procedimiento de reinicio en caso de falla del sistema. f) Documentar los contactos de los diferentes clientes en caso de incidentes. g) Documentar el proceso de reimpresión de páginas de prueba. h) Documentar la configuración del explorador para el uso del sistema por parte del cliente.
Gestión del cambio	
	a) Identificación y registro de los cambios significativos. b) Planificación y prueba de cambios. c) Evaluación de los posibles impactos, incluyendo los impactos de la seguridad de la información. d) Se debe crear un procedimiento de aprobación formal para los cambios que se desean realizar. e) Comunicar los detalles del cambio al personal relevante. f) Verificación de que se han cumplido los requisitos de seguridad de la información. g) Designar responsables del control de cambios en los equipos y software.
Gestión de capacidades	
	a) Realizar la eliminación de datos obsoletos para generar más espacio en disco. b) Optimizar los procesos y programas a través de lotes. c) Optimizar la lógica de la aplicación y automatizar las consultas a la base de datos. d) Restringir el ancho de banda en especial a los servicios que consumen muchos recursos si no son importantes y críticos para el negocio.

Separación de entornos de desarrollo, pruebas, producción y capacitación	
	a) Se deben documentar las reglas para la transferencia de software desde el ambiente de desarrollo al ambiente de producción. b) Aislar los ambientes de desarrollo, pruebas, producción y capacitación. c) Para realizar cambios en los sistemas de producción deben probarse en un entorno de prueba antes de ser aplicados a producción. d) Crear un ambiente de pruebas semejante al ambiente de producción. e) Los ambientes de desarrollo y producción deben ejecutarse en diferentes sistemas, dominios o directorios. f) Se deben definir diferentes perfiles de usuario para los ambientes de desarrollo, pruebas, y producción. g) En los ambientes de prueba no se deben copiar los datos confidenciales. h) Se debe solicitar una autorización previa cuando el personal de desarrollo necesita acceso al ambiente de producción únicamente en caso de extrema necesidad.
Objetivo de control: Protección contra código malicioso	
Protección contra el código malicioso	
	a) Prohibir el uso de software no autorizado en Soft Warehouse S.A. • Realizar un listado de software autorizado. b) Actualizar con la última versión a los sistemas operativos y sistemas de procesamiento de información. c) Instalar y actualizar los ordenadores que no posean software de antivirus y contra código malicioso. d) Realizar planes de continuidad para recuperarse de ataques de malware incluyendo los arreglos necesarios de respaldo y recuperación de datos y software. e) Realizar procedimientos para recopilar regularmente información acerca de sitios web que brindan información sobre nuevo malware. f) Realizar afiches informativos acerca de los virus y código malicioso. • Sitios de internet confiables. • Proveedores que producen software de protección contra malware. g) Concientizar al personal acerca de la influencia de los virus y cómo actuar frente a esta amenaza.
Objetivo de control: Copia de Seguridad	
Copia de seguridad de la información	
	a) Establecer normas de etiquetado para las copias de seguridad marcando su contenido, fecha y retención. b) De acuerdo a los requisitos de Soft Warehouse S.A. se debe definir la extensión y la frecuencia de los respaldos. • Extensión (completo/diferencial). • Frecuencia (días/ meses / años). c) La copia de seguridad debe tener registros precisos y completos y procedimientos de restauración documentados. d) Las copias de seguridad deben almacenarse en una ubicación remota. e) Las copias de seguridad deben protegerse mediante cifrado. f) Definir procedimientos de las copias de seguridad en el momento en que concluye su vida útil.

	g) Probar la capacidad de restauración de datos respaldados realizado en ambientes de prueba, no sobrescrito en el ambiente de producción. h) Los medios de respaldo se deben probar con regularidad para asegurar que se pueden usar en caso de emergencia o cuando sea necesario.
Objetivo de control: Registro y monitoreo	
Registro de eventos	
	a) Realizar registros de ID de usuario. b) Realizar registros de actividad del sistema. c) Realizar registros fechas, horas y detalles de eventos clave (inicio de sesión y cierre de sesión) d) Realizar registros de intentos de accesos satisfactorios y rechazos del sistema. e) Realizar registros de cambios de la configuración del sistema. f) Realizar registros de uso de utilidades y aplicaciones del sistema. g) Realizar registros de direcciones de red y protocolos. h) Realizar registros de alarmas planeadas por el sistema de control de accesos. i) Realizar registros de transacciones realizadas por los usuarios en los diferentes ambientes.
Protección del registro de la información	
	a) Proteger las alteraciones en los tipos de mensajes que se registran. b) Proteger los archivos de registros que se están editando o eliminando. c) Verificar la capacidad de almacenamiento de los medios de registro.
Registro de actividad del administrador y operador del sistema	
	a) Mantener el registro con la siguiente información: • La hora en la que ocurrió el evento. • Información detallada del evento. • La cuenta de administrador y el usuario responsable. • Procesos relacionados.
Sincronización del reloj	
	a) Sincronizar los relojes de los sistemas de procesamiento de información en base a un protocolo o servicio de tiempo de red para mantenerlos sincronizados en un tiempo exacto. b) Monitorear la configuración de los relojes para una mejor exactitud en los registros de auditoria. c) Considerar las especificaciones locales para reajustar la fecha y hora por ejemplo (ubicación geográfica) en el caso de que se les de soporte a clientes de otros países. d) Mantener una configuración correcta de los relojes para obtener registros precisos.
Objetivo de Control: Control del software de explotación	
Instalación de software en sistemas de producción	
	a) El ambiente de producción solo debe implementarse después de extensas pruebas exitosas. • Las pruebas deben cubrir usabilidad, seguridad, efectos en otros sistemas, y confiabilidad.

	b) Los ambientes de producción solo deben contener el código ejecutable aprobado y no el código de desarrollo. c) Definir una estrategia de revisión antes de implementar los cambios. d) Mantener un registro de auditoria de todas las actualizaciones que se realizan en el ambiente de producción. e) Las versiones anteriores de los ambientes de producción deben conservarse como una medida de contingencia. f) Las versiones anteriores de los ambientes de producción se deben archivar con toda la información, los parámetros necesarios, procedimientos y detalles de configuración.
Objetivo de Control: Gestión de la vulnerabilidad técnica	
Gestión de las vulnerabilidades técnicas	
	a) Cuando se identifica una vulnerabilidad técnica, Soft Warehouse S.A. debe identificar los riesgos asociados y las acciones a tomar. • Las acciones que se van a tomar deben llevarse a cabo de acuerdo a los controles relacionados con la gestión del cambio o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información. • La gestión de vulnerabilidades debe ser monitoreado y evaluado regularmente. b) Los parches deben aprobarse y evaluarse antes de su instalación para garantizar su eficiencia y efectividad.
Restricciones en la instalación de software	
	a) Identificar qué tipo de instalaciones de software es permitido como por ejemplo (actualizaciones y parches de seguridad) b) Identificar qué tipo de instalaciones son prohibidas como por ejemplo (software solo para uso personal). c) Los privilegios de instalación se deben otorgar teniendo en cuenta el rol del usuario involucrado.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**SEGURIDAD DE LAS COMUNICACIONES**
OBJETIVO	Garantizar la protección de la información en las redes que maneja Soft Warehouse S.A.

Objetivo de Control: Gestión de seguridad en las redes.	
Control de red	
	a) Designar responsables y diseñar procedimientos que maneja la gestión de las redes. b) Se deben establecer controles para salvaguardar la confidencialidad e integridad de los datos por medio del re-direccionamiento de puertos y accesos por VPNs. c) Los sistemas de red deben ser autentificados. d) La conexión de los sistemas de red debe estar restringida. e) Monitorizar apropiada para la detección de acciones que puedan afectar la continuidad del sistema. f) Disponer de documentación del esquema de redes de los enlaces de datos, Internet y redes locales de Soft Warehouse S.A. g) Diseñar controles para salvaguardar la confidencialidad e integridad de los datos que se transmiten a partir de redes públicas o redes inalámbricas.
Mecanismos de seguridad asociados a servicios de red.	
	a) Incorporar tecnología para la seguridad de los servicios de red como autentificación, encriptación, controles de conexión. b) Diseñar procedimientos que restrinja el acceso a servicios o aplicaciones de red donde sea necesario. c) Definir los parámetros técnicos necesarios para la conexión segura con los servidores de red de acuerdo con las reglas de seguridad y conexiones de red.
Segregación de redes	
	a) Dividir la red en dominios de red separadas. • Los dominios se pueden elegir en función a los niveles de confianza por ejemplo (dominio de acceso público, acceso al servidor, acceso a los ambientes). b) El perímetro de cada dominio debe estar bien definido utilizando puertas de enlace como por ejemplo (cortafuegos, enrutador de filtrado) c) Las redes inalámbricas requieren un tratamiento especial debido a un perímetro de red definido.
Objetivo de Control: Intercambio de información con partes externas	
Políticas y procedimientos de intercambio de información	

	a) Definir procedimientos diseñados para proteger la información intercambiada contra la copia, modificación, desvió y destrucción. b) Diseñar procedimientos que permitan la detección y protección contra malware. c) Establecer procedimientos para proteger la información electrónica sensible. d) Uso de técnicas criptográficas por ejemplo para proteger la confidencialidad, integridad y autenticidad de información. e) Concientizar al personal de tomar precauciones apropiadas para no revelar información confidencial. f) No dejar información sensible en copiadoras, impresoras, mesas de escritorio. g) No revelar información confidencial mientras se mantiene una llamada telefónica. h) No dejar mensajes que contengan información confidencial en contestadoras ya que pueden ser usadas por personas que no están autorizadas.
Acuerdos de intercambio	
	a) Definir responsabilidades de gestión para controlar y notificar la transmisión, el envío y la recepción. b) Definir procedimientos para asegurar que la trazabilidad y el no repudio. c) Establecer normas técnicas mínimas para el embalaje y la transmisión de segura de información. d) Acordar responsabilidades en caso de incidentes de seguridad de la información, como por ejemplo la pérdida de datos. e) Hacer uso de un sistema de etiquetado para la información delicada o critica, teniendo en cuenta que las etiquetas deben ser legibles. f) Mantener una cadena de custodia para la información que se encuentra en tránsito.
Mensajería instantánea	
	a) Asegurar el direccionamiento correcto y el transporte del mensaje. b) Mantener la fiabilidad y disponibilidad del servicio. c) Disponer de niveles fuertes de autentificación que controlen el acceso desde redes de acceso público.
Acuerdos de confidencialidad y secreto	
	a) Considerar la duración prevista de un acuerdo, incluidos los casos en que podría ser necesario mantener la confidencialidad. b) Definir las acciones necesarias cuando se termina un acuerdo. c) Establecer los términos para que la información sea devuelta o destruida al momento en el que cese el contrato. d) Los acuerdos de confidencialidad deben ser firmados por todo el personal de Soft Warehouse S.A. sin excepciones. e) Determinar la información que debe protegerse como por ejemplo información confidencial. f) Detallar las acciones que se deben tomar en caso de incumplimiento del acuerdo.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**
OBJETIVO	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información de Soft Warehouse S.A.

Objetivo de Control: Requisitos de seguridad de los sistemas de información.	
Análisis y especificación de los requisitos de seguridad de la información	
	a) Establecer los requerimientos de seguridad como por ejemplo (criptografía, control de sesiones). b) Informar a los usuarios y operadores de sus deberes y responsabilidades. c) Definir los requerimientos de seguridad y los controles requeridos teniendo en cuenta el costo y daño que pudiera ocasionar una falla de seguridad. d) Considerar las necesidades de protección requerida de los activos involucrados con relación a la disponibilidad, confidencialidad e integridad.
Protección de las transacciones por redes telemáticas	
	a) Considerar el uso de firmas electrónicas por cada una de las partes involucradas. b) La ruta de comunicaciones entre todas las partes involucrados esta encriptada. c) Adoptar medidas de protección a los protocolos que son utilizados para comunicarse con las partes involucradas.
Objetivo de Control: Seguridad en los procesos de desarrollo y soporte	
Política de desarrollo seguro de software	
	a) Considerar el uso de entornos de desarrollo seguros. b) Mantener la seguridad en el ciclo de vida del desarrollo de software. • Seguridad en la metodología de software. • Pautas de codificación segura para cada lenguaje de programación utilizado. c) Definir requisitos de seguridad en la fase de diseño. d) Utilización de repositorios seguros. e) Enfatizar la seguridad en el control de versiones. f) Concientizar al personal acerca de los requerimientos de seguridad en las aplicaciones. g) Definir puntos de control de seguridad dentro de los hitos del proyecto. h) Fomentar la capacidad de los desarrolladores de evitar, encontrar y corregir vulnerabilidades.
Procedimientos de control de cambio del sistema	
	a) Asegurar que los cambios sean enviados por usuarios autorizados.

	b) Revisar los controles y los procedimientos de integridad para garantizar que no se vean comprometidos por los cambios. c) Identificar y verificar el código crítico de seguridad para minimizar la probabilidad de debilidades de seguridad conocidas. d) Garantizar que los usuarios autorizados acepten los cambios antes de la implementación. e) Mantener un control de versión para todas las actualizaciones de software. f) Garantizar que la implementación de los cambios tenga lugar en el momento adecuado y no perturbe los procesos de negocio.
Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	
	a) Revisión de los procedimientos de control e integridad de la aplicación para garantizar que no se hayan visto comprometidos por los cambios en el sistema operativo. b) Asegurar que la notificación de los cambios de la plataforma operativa se proporcione a tiempo para permitir pruebas y revisiones antes de la implementación. c) Garantizar que se realicen los cambios apropiados en los planes de continuidad del negocio.
Restricciones a los cambios en los paquetes de software	
	a) Compatibilidad con otro software en uso. b) Consentimiento del vendedor del paquete de software. c) Riesgo de que los cambios que son integrados se vean comprometidos. d) Cambios requeridos del vendedor como actualizaciones estándar del programa
Entorno de desarrollo seguro	
	a) Asegurar que los datos con los que cuenta el entorno provengan de fuentes confiables y se mantenga su integridad durante todo el ciclo de vida en el sistema. b) Requisitos externos e internos aplicables, por ejemplo, de reglamentos o políticas. c) Control de acceso al entorno de desarrollo. d) Las copias de seguridad se almacenan en ubicaciones fuera del sitio. e) Segregación entre diferentes entorno de desarrollo. f) Monitoreo del cambio en el entorno y el código almacenado en el mismo. g) Confiabilidad en el personal que trabaja en el entorno. h) Control sobre el movimiento de datos desde y hacia el entorno.
Pruebas de aceptación	
	a) Usar herramientas automatizadas para el análisis de código o escáneres de vulnerabilidad para el análisis de defectos. b) Las pruebas deben realizarse en un entorno de prueba realista para garantizar que el sistema no introduzca vulnerabilidades al entorno de la Soft Warehouse S.A. y que pruebas son confiables.
Pruebas de funcionalidad durante el desarrollo de los sistemas	
	a) Los sistemas nuevos y actualizados requieren pruebas y verificaciones exhaustivas durante los procesos de desarrollo.

	b) Las pruebas de funcionalidad deben ser realizadas por el equipo de desarrollo. c) El alcance de las pruebas debe ser proporcional a la importancia y naturaleza del sistema.
Objetivo de Control: Datos de prueba	
Protección de los datos usados en las pruebas	
	a) Pedir una autorización por separado cada vez que se realice una copia de datos en un entorno de prueba. b) Realizar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción. c) Modificar los datos en el ambiente de pruebas para conseguir resultados satisfactorios d) Eliminar inmediatamente, una vez completadas las pruebas, la información de producción

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**RELACIONES CON PROVEEDORES**
OBJETIVO	Garantizar la protección de los activos de Soft Warehouse S.A. a la que pueden acceder los proveedores.

Objetivo de Control: Seguridad de la información en las relaciones con proveedores	
Política de seguridad de la información para proveedores	
	a) Identificar y documentar los tipos de proveedores, por ejemplo, servicios de TI, servicios logísticos, servicios financieros, componentes de infraestructura de TI, a quienes la compañía permitirá acceder a su información. b) Definir un proceso para gestionar las relaciones con los proveedores. c) Definir procesos y procedimientos para monitorear el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso. d) Manejar incidentes y contingencias asociados con el acceso del proveedor, incluidas las responsabilidades tanto la compañía como los proveedores. e) Concientización para el personal de Soft Warehouse S.A. que interactúa con el proveedor con respecto a reglas apropiadas de compromiso y comportamiento basadas en el tipo de proveedor y el nivel de acceso del proveedor a los sistemas e información de la compañía. f) Definir acuerdos sobre niveles de servicio de soporte y mantenimiento con el proveedor.
Tratamiento del riesgo dentro de acuerdos con proveedores	
	a) Definir métodos para proporcionar o acceder a la información. b) Clasificar la información de acuerdo con el esquema de clasificación Soft Warehouse S.A. c) Considerar los requisitos legales y reglamentarios, incluida la protección de datos, derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se garantizará que se cumplan. d) Definir políticas de seguridad de la información relevantes para el contrato con el proveedor. e) Derecho a auditar los procesos y controles del proveedor relacionados con el acuerdo. f) Obligación del proveedor de entregar periódicamente un informe independiente sobre la efectividad de los controles y acuerdos de servicio planteados en el contrato.
Objetivos de Control: Gestión de la prestación del servicio por parte de los proveedores	
Supervisión y revisión de los servicios prestados por terceros	

	a) Hacer un seguimiento del desempeño del servicio y comparar con los acuerdos de cumplimiento. b) Establecer reuniones y discutir acerca de los informes extraídos del funcionamiento del servicio prestado por terceras partes. c) Proporcionar información sobre incidentes de seguridad de la información y revisar esta información según sea necesario. d) Resolver y gestionar cualquier problema identificado. e) Revisar los aspectos de seguridad de la información con el proveedor. f) Asegurarse que el proveedor mantenga suficiente capacidad de servicio para mantener los niveles de continuidad.
Gestión de cambios de los servicios prestados por terceros	
	a) Gestionar cambios en los acuerdos con los proveedores. b) Gestionar los cambios realizados en la organización para implementar: • Mejoras a los servicios ofrecidos. • Desarrollo de nuevas aplicaciones y sistemas. • Modificaciones o actualizaciones de las políticas y procedimientos de Soft Warehouse S.A. • Controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad. c) Gestionar cambios en los servicios del proveedor para implementar: • Cambios realizados y mejoras a las redes. • El uso de nuevas tecnologías. • Adoptar nuevos productos o versiones. • Integrar nuevas herramientas y adopción de entornos de desarrollo. • Cambios en la ubicación física de las instalaciones de servicio.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
OBJETIVO	Crear un ambiente adecuado de seguridad de la información, incluyendo la comunicación de los incidentes al personal de Soft Warehouse S.A.

Objetivo de Control: Gestión de incidentes de seguridad de la información.	
Notificación de los eventos de seguridad de la información	
	a) Infracción de la integridad de la información, confidencialidad o disponibilidad. b) Errores humanos. c) Incumplimientos con políticas o directrices. d) Incumplimientos de las disposiciones de seguridad física. e) Cambios en el sistema no controlados. f) Mal funcionamiento del software o hardware. g) Violaciones de acceso.
Respuesta a los incidentes de seguridad de la información	
	a) Recolectar evidencia tan pronto como sea posible después de la ocurrencia. b) Realizar análisis forenses de seguridad de la información, según sea necesario. c) Asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para su posterior análisis. d) Comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante e) Tratar con debilidades de seguridad de la información que se haya encontrado que causan o contribuyen al incidente. f) Una vez que el incidente ha sido tratado exitosamente, hay que proceder a cerrarlo formalmente y registrarlo.
Aprendizaje de los incidentes de seguridad de la información	
	a) Los datos obtenidos a partir de la evaluación de los incidentes deben ser parte de una base de conocimiento para identificar cuáles son los incidentes más recurrentes y como solucionarlo. b) Listar el número de incidentes por tipo y de acuerdo al tiempo de resolución. c) Determinar el costo promedio por incidente. d) Determinar el número de incidentes recurrentes. e) Determinar la frecuencia de un incidente recurrente.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
OBJETIVO	Gestionar la continuidad del negocio para reducir a niveles aceptables, las interrupciones causadas por desastres y fallos de seguridad en Soft Warehouse S.A.

Objetivo de Control: Continuidad de la seguridad de la información	
Planificación de la continuidad de la seguridad de la información	
	a) El Responsable del área de Tecnologías de la Información será designado como coordinador de la continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad, así como de la seguridad del personal. b) Elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad.
Implantación de la continuidad de la seguridad de la información	
	a) Contar con personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para administrar un incidente y mantener la seguridad de la información. b) Desarrollar planes documentados, procedimientos de respuesta y recuperación, detallando cómo Soft Warehouse S.A. gestionará un incidente y mantendrá su seguridad de la información en un nivel estable. c) Definir qué tipo de mensaje se debe trasmitir en caso de un desastre o fallo de seguridad.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	
	a) Realizar un análisis de los procesos de continuidad de seguridad de la información de Soft Warehouse S.A. para analizar su funcionamiento y eficacia en el entorno empresarial. b) Realizar la validación y efectividad de las pautas tomadas para la continuidad de la seguridad de la información frente a desastres. Realizar pruebas de: a. Validez: revisar y discutir el plan. b. Simulación: escenario donde se pueda verificar el plan de continuidad. c. Actividades críticas: pruebas en un entorno controlado. d. Completa: interrupción real y aplicación del plan de continuidad. c) Ejecutar el plan de continuidad, estrategias y procesos generados.

	d) La revisión del plan de continuidad de Soft Warehouse S.A. debe realizarse anualmente.
Objetivo de Control: Redundancias	
Disponibilidad de instalaciones para el procesamiento de información	
	a) Identificar los requisitos comerciales para la disponibilidad de los sistemas de información. b) No se debe utilizar la arquitectura del sistema existente, componentes redundantes. c) Los sistemas de información redundantes deben ser probados para asegurar que los componentes funcionan según lo previsto. d) La implementación de redundancias puede introducir riesgos de integridad o confidencialidad de la información que deben tenerse en cuenta al diseñar sistemas de información.

SEGURIDAD DE LA INFORMACIÓN	
DOMINIO	**CUMPLIMIENTO**
OBJETIVO	Evitar incumplimientos de las obligaciones legales, normativas, leyes relacionadas con la seguridad de la información, y el Estado.

Objetivo de Control: Cumplimiento de los requisitos legales y contractuales	
Identificación de la legislación aplicable	
	a) Realizar un inventario de las normas legales, reglamentarias y contractuales para cada activo de información que utiliza la Soft Warehouse S.A. b) Considerar las normas y leyes relacionadas con la gestión de los datos e información electrónica. • Constitución de la República del Ecuador. • Leyes y normas de control del sistema financiero. • Superintendencia de Economía Popular y Solidaria. • Ley Orgánica de Transparencia y Acceso a la Información Pública. • Ley de economía popular y solidaria. • Código Ingenios • Decreto Ejecutivo No.1014 sobre el uso de software libre.
Derechos de propiedad intelectual	
	a) Adquirir software a través de fuentes conocidas y de buena reputación, para garantizar que no se viole el derecho de autor. b) Mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual y notificar el incumplimiento para tomar medidas disciplinarias contra la persona que las irrespete. c) Llevar a cabo revisiones donde solo se instale software autorizado y productos con licencia. d) Tener en cuenta el número máximo de usuarios que permite la licencia del software. e) Cumplir con los términos y condiciones del software. f) No copiar código, total o parcialmente, libros, artículos u otros documentos que no están permitidos por el autor. g) No duplicar, convertir a otro formato o extraer de grabaciones comerciales (película, audio) aparte de lo permitido por la ley de derechos de autor.
Protección de los registros de la compañía	
	a) Se deben emitir directrices sobre la retención, almacenamiento, manejo y eliminación de registros e información.

	b) Se debe elaborar un cronograma de retención que identifique los registros y el período de tiempo durante el cual deben ser retenidos en Soft Warehouse S.A. c) Se debe mantener un inventario de las fuentes de información claves. d) Implementar controles apropiados para proteger los registros contra pérdida, destrucción y falsificación de la información.
Objetivo de Control: Revisiones de la seguridad de la información	
Cumplimiento de las políticas y normas de seguridad	
	a) Identificar las causas del incumplimiento. b) Evaluar la necesidad de acciones para lograr el cumplimiento. c) Implementar la acción correctiva apropiada. d) Llevar el control de las normas de seguridad tomadas con el fin de saber si son efectivas e identificar posibles deficiencias y debilidades.

Glosario de Términos

Término	Definición
Activo	Se considera un bien que posee una organización.
Calidad	Una actividad o proceso probado que se ha puesto en práctica con éxito por múltiples empresas y se ha demostrado que produce resultados fiables.
Continuidad de negocio	Evitar, mitigar y recuperarse de una interrupción, se enfocan en aspectos de recuperación dentro de la continuidad.
Control	Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal.
Comité de Gestión de Seguridad de la Información	Es un cuerpo integrado por miembros de cada área de la compañía, con el fin de garantizar el apoyo hacia la seguridad de la información de la misma.
Cultura	Un patrón de comportamientos, creencias, hipótesis, actitudes y formas de hacer las cosas.
Estructura organizativa	Es la forma en la que una empresa se va a gestionar, sus estructuras, jerarquías y dependencias.
Gestión	Incluye el uso juicioso de medios (recursos, personas, procesos, prácticas, etc.) para conseguir un fin identificado. La gestión se refiere a las actividades operacionales de planificación, construcción, organización y control.
Información	Un activo que es esencial para el negocio de una organización. Puede existir de muchas formas: impreso o escrito en papel, almacenado electrónicamente, trasmitido por correo o de forma electrónica o hablada durante una organización.
Objetivo	Declaración de un resultado deseado.
Oficial de Seguridad de la información	Profesional especializado en prevenir delitos informáticos su función principal es alinear la seguridad de la información con los objetivos de negocio de tal manera que la información de la organización se encuentre protegida.
Política	Son instrumentos que nos permiten comunicar las reglas de la empresa.
Proceso	Una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de fuentes (incluyente otros procesos), manipula esas entradas y genera salidas (por ejemplo, productos, servicios).
Sistemas de información	Está compuesto de hardware, software, servicios públicos y todos los diversos componentes necesarios para construir un sistema para gestionar información de manera adecuada.

*La mayoría de los términos fueron tomados de:
(Cobit 5, Un Marco de Negocio para el Gobierno y Gestion de TI de la empresa, 2012)